# Utah Governance, Risk, and Compliance

**Last updated: 04/03/2024**

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Some examples and graphics depicted herein are provided for illustration only. No real association or connection to ServiceNow products or services is intended or should be inferred.

ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

Please read the ServiceNow Website Terms of Use at www.servicenow.com/terms-of-use.html

Company Headquarters
2225 Lawson Lane
Santa Clara, CA 95054
United States
(408) 501-8550

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

servicenow

# Table of Contents


Governance, Risk, and Compliance ..... 6
GRC and the ServiceNow Store ..... 11
Download a GRC application from the ServiceNow Store for the first time ..... 12
Install GRC content packs and integrations ..... 18
Update a GRC application previously downloaded from the ServiceNow Store ..... 19
Upgrade your instance to the next GRC family release ..... 19
Audit Management ..... 19
GRC Audit Management implementation ..... 20
Audit Management workspace ..... 30
Understanding Audit Management ..... 69
Evidence request ..... 124
Audit plan overview ..... 133
Manage milestones ..... 145
Integration of Audit Management with Time Card management ..... 147
Audit observations ..... 148
Roll up expenses and resources in an engagement ..... 150
Roles required for Engagement project planning for Project Portfolio Management ..... 151
Roles required for Advanced planning capability and Project Portfolio Management integration ..... 153
Business Continuity Management ..... 155
Exploring Business Continuity Management ..... 157
Configuring Business Continuity Management ..... 201
Managing business continuity workflow tasks in BCM UIB Workspace ..... 277
Sending notifications with Everbridge in BCM Configurable Workspace ..... 364
Using BCM classic Workspace ..... 368
Business Continuity Management reference ..... 456
Compliance Case Management ..... 477
Exploring Compliance Case Management ..... 478
Configuring Compliance Case Management ..... 490
Using Compliance Case Management ..... 503
Compliance Case Management reference ..... 527
Continuous Authorization and Monitoring ..... 530
Understanding Continuous Authorization and Monitoring ..... 531
Continuous Authorization and Monitoring implementation ..... 532
Prepare the authorization package ..... 536
Categorize the authorization package ..... 541
Select controls for an authorization package ..... 543
Implement controls ..... 549
Assess, authorize, monitor, and generate reports ..... 550



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Understanding assessment objectives in CAM....553
Continuous Authorization and Monitoring overview reports....571
Operational Resilience....577
Exploring Operational Resilience....578
Configuring Operational Resilience....581
Setting up the features and capabilities in classic Operational Resilience....605
Setting up the features in Operational Resilience Workspace....658
Displaying reports in Operational Resilience....750
Operational Resilience reference....764
Policy and Compliance Management....775
Exploring Policy and Compliance Management....776
Implementing Policy and Compliance Management....779
Using the Classic user interface for Policy and Compliance tasks....864
Performing compliance tasks in Compliance Workspace....973
Policy authoring and redlining in Compliance Workspace....1065
Set up the dynamic approval configuration on a policy record....1076
Managing GRC tasks from Employee Center....1085
360° Relationship Visualization for Policy and Compliance Management....1096
GRC: Policy and Compliance integrator....1098
Policy as Code Engine for Preventive compliance management....1111
DevOps accelerator for control compliance, PaCE execution, and exception management....1115
Manage continuous monitoring for controls between Configuration Compliance and Policy and Compliance Management....1117
Policy and Compliance Management reference....1119
Analytics and Reporting solutions for GRC: Policy and Compliance Management....1130
Privacy Management....1134
Exploring Privacy Management....1134
Configuring Privacy Management....1147
Using Privacy Management....1158
Integrating Employee Center and Risk portal with Privacy Management....1177
Privacy Case Management....1178
Privacy Management reference....1218
Reporting for Privacy Management....1227
Regulatory Change Management....1234
Exploring Regulatory Change Management application....1235
Setup checklist for Regulatory Change Management....1242
Regulatory Change Management application in the Compliance Workspace....1243
Regulatory Change Management classic user interface....1269
Risk Management....1297
Exploring Risk Management....1299
Configuring Risk Management....1347

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Integrating Risk Management with other applications....1365
Using Risk Management....1398
Using the Risk Workspace....1562
GRC: Metrics in Integrated Risk Management....1633
Analytics and reporting solutions for Risk Management....1680
Risk Management reference....1715
Third-party Risk Management....1731
Exploring Third-party Risk Management....1732
Configuring Third-party Risk Management....1751
Requesting third-party risk due diligence....1808
Assessing your third-party risk....1812
Monitoring your third-party risk....1827
Approving or rejecting requests for due diligence....1855
Managing the contract risk process....1858
Working in the VRM Classic user interface....1867
Managing the Third-party portal....1891
Integrating scores from risk intelligence providers....1900
Third-party Risk Management reference....1910
Common GRC features....1947
Mobile experience for Governance, Risk, and Compliance....1947
GRC application nomenclature updates and industry terminology....1947
GRC content packs....1960
GRC integrations....1978
GRC use case accelerators....1990
360° Relationship Visualization....2148
Using the item generation process to generate controls and risks....2162
Approval configuration....2174
Confidential records....2179
User hierarchy....2188
User group-based access on the GRC tables....2192
Content references in GRC....2193
Manage issues....2199
Domain separation in GRC....2207
Breadcrumb navigation....2210
Taxonomy management in GRC....2210
Landing Page Configurations module....2211
My tasks in the workspace....2220
Exploring the entities....2222
Viewing and updating Governance, Risk, and Compliance exceptions....2253
Advanced Governance, Risk, and Compliance Application Risk dashboard....2254

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

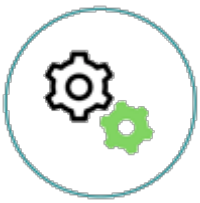
# Governance, Risk, and Compliance

Respond to business risks in real time. Connect security and IT with an integrated risk program offering continuous monitoring, prioritization, and automation.

### Governance, Risk, and Compliance applications

| | | |
|---|---|---|
| Audit Management<br>  <br>Use risk data to scope and prioritize audit plans and automate cross-functional processes. | Business Continuity Management<br>  <br>Plan, exercise, and recover from disasters effectively and efficiently. | Compliance Case Management<br>  <br>Report, investigate, analyze, and resolve compliance cases. |
| Continuous Authorization and Monitoring<br>  <br>Accelerate the process of bringing IT systems online and continuously monitoring them. | Operational Resilience<br>  <br>Gain real-time visibility into the resilience of your technology, people, processes, and facilities. | Policy and Compliance Management<br>  <br>Automate and manage policy life-cycles and continuously monitor for compliance. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| | | |
|---|---|---|
| Privacy Management<br>  <br>Manage privacy risk and compliance across the enterprise in real time. | Regulatory Change Management<br>  <br>Keep pace with today's complex regulatory landscape with integration to leading content providers. | Risk Management<br>  <br>Enable fine-grained business impact analysis to appropriately prioritize and respond to risks. |
| Third-party Risk Management<br>  <br>Continuously monitor, detect, assess, mitigate, and remediate risks in third-party ecosystems. | **Common** GRC **features**<br>  <br>Leverage the power of entities, 360 degree views, the tasks landing page, and security features across GRC products. | |

## Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

## Respond to business risks in real time with ServiceNow GRC

ServiceNow Governance, Risk, and Compliance (GRC) helps transform inefficient processes across your extended enterprise into an integrated risk program. Through continuous monitoring and automation, the GRC applications deliver a real time view of compliance and risk, improve decision making, and increase performance across your organization and with vendors.

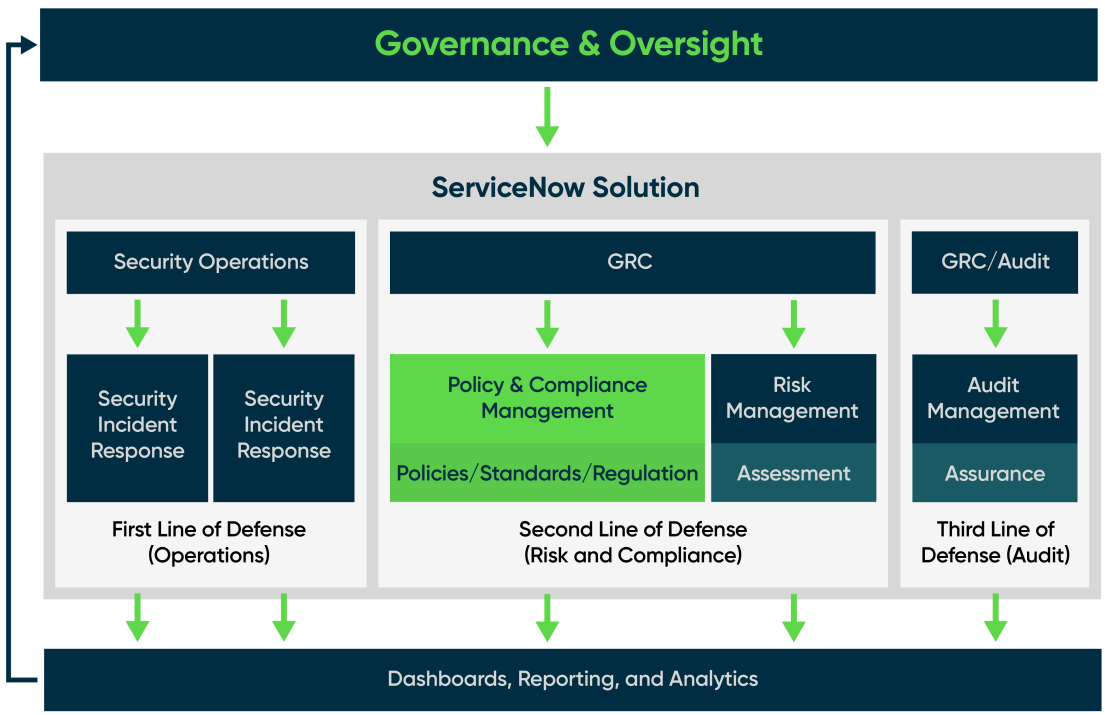
Only ServiceNow applications can connect the business, security, and IT with an integrated risk framework that transforms manual, siloed, and inefficient processes into a unified program that is built on a single platform.

View and download the full info card for a highlight of GRC features.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| | |
|---|---|
| | Streamline and automate activities in the face of an emergency<br><br>Mobilize your business continuity efforts during natural disasters and pandemics like COVID-19. |
| | Automate and manage policy life cycles and continuously monitor for compliance.<br><br>It makes perfect sense to embrace a single platform that can make all compliance efforts more organized, simpler, more transparent, and highly reliable. |
| | Enable fine-grained business impact analysis to appropriately prioritize and respond to risks.<br><br>Respond to business risks in real-time with integrated risk management. |
| | Use risk data to scope and prioritize audit plans and automate cross-functional processes.<br><br>Reduce audit costs, improve efficiency, and minimize risk. |
| | Continuously monitor, detect, assess, mitigate, and remediate risk in vendor ecosystems.<br><br>As your vendors become privy to more of your sensitive systems and data, their risk and compliance posture becomes even more important to your security. It's important to assess your vendors regularly and proactively mitigate any issues that arise. |

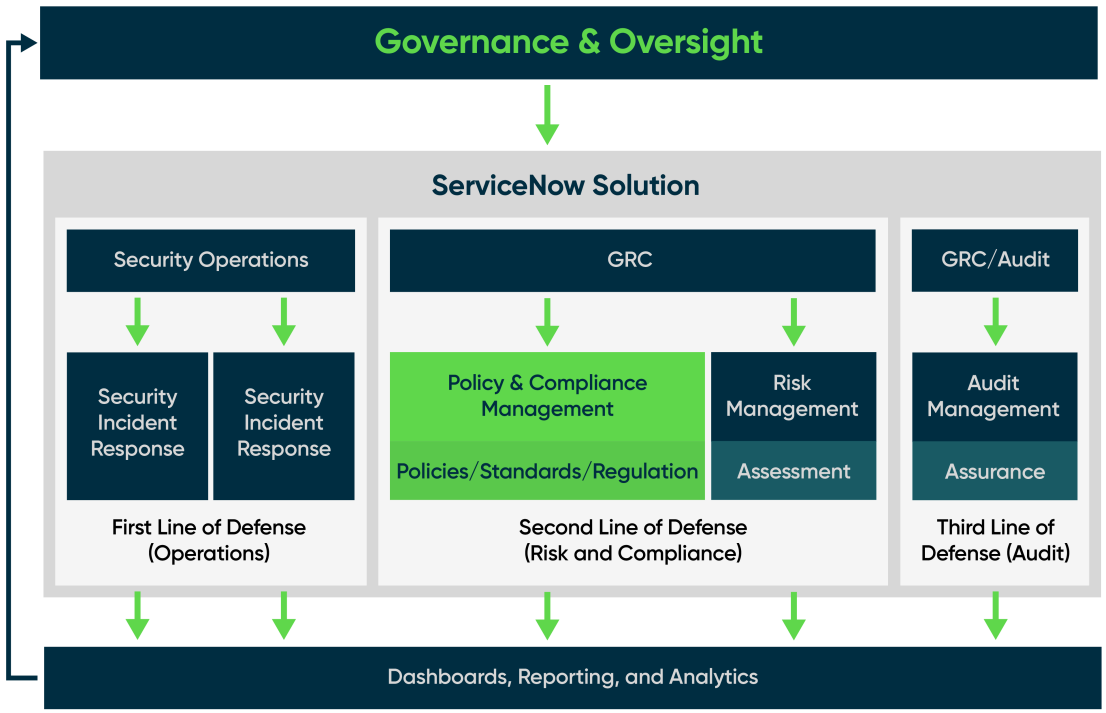
## Automate and manage policy life cycles and continuously monitor for compliance




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The ServiceNow® Policy and Compliance Management product provides a centralized process for creating and managing policies, standards, and internal control procedures. The process automatically cross-maps the procedures to external regulations. Also, the application provides structured workflows for the identification, assessment, and continuous monitoring of control activities.

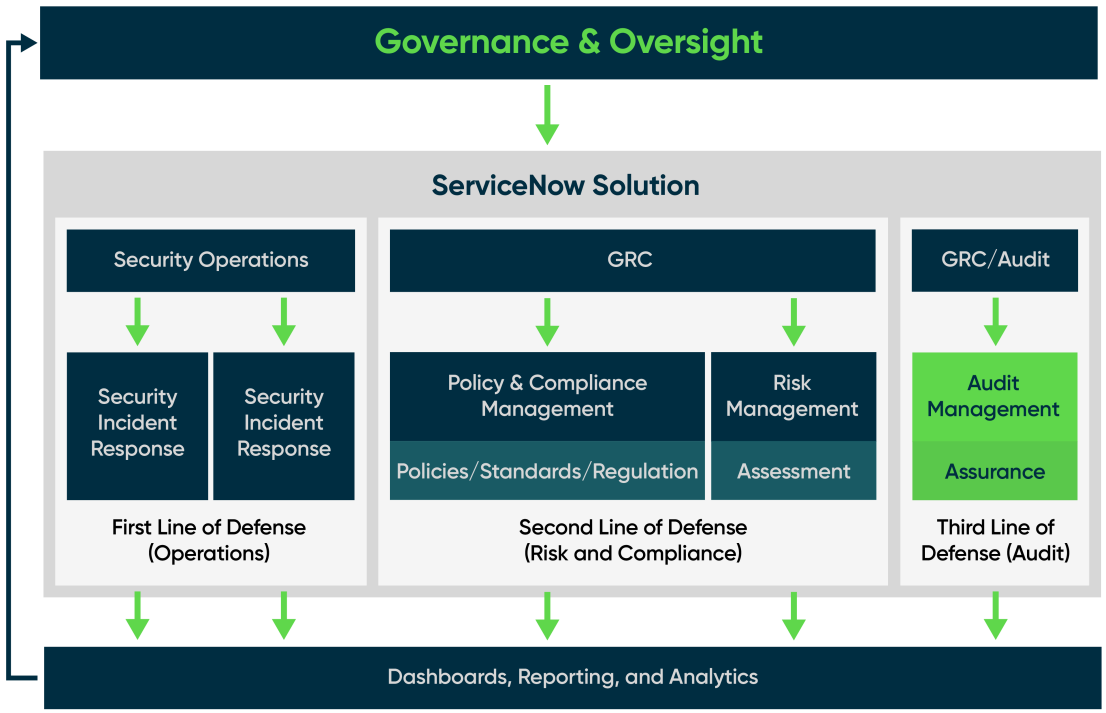
## Enable fine-grained business impact analysis to appropriately prioritize and respond to risks




The ServiceNow Risk Management product provides a centralized process to identify, assess, respond to, and continuously monitor Enterprise and IT risks that may negatively impact business operations. The application also provides structured workflows for the management of risk assessments, risk indicators, and risk issues.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Use risk data to scope and prioritize audit plans and automate cross-functional processes




The ServiceNow Audit Management product automates the work streams of internal audits teams, optimizing resources and productivity, and eliminating recurring audit findings. Audit Management uses compliance and risk data to scope, plan, and prioritize audit engagements. The ongoing review of policies and procedures, risks, and control breakdowns provide an opportunity for fixing issues before they become audit failures.

The ServiceNow Regulatory Change Management application empowers the customers to check upcoming regulatory changes, assess their impact, and implement risk and compliance related changes, ensuring overall regulatory compliance.

## Continuously monitor, detect, assess, mitigate, and remediate risk in vendor ecosystems

As your vendors become privy to more of your sensitive systems and data, their risk and compliance posture becomes even more important to your security. It's important to assess your vendors regularly, but until now, it has been a time-consuming and error-prone exercise comprised of spreadsheets, email, and rudimentary legacy risk management tools.

The Vendor Risk Management application transforms the way you manage vendor risk through vital reporting of vendor risk and issues, a consistent assessment and remediation process, and automated assessment procedures. It provides a means to facilitate stakeholder interactions, drive transparency and accountability, and effectively monitor vendor-related risks.

By aligning Vendor Risk Management with overall enterprise risk management priorities, you can create an essential integrated view of risk and a stronger extended enterprise risk posture.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Learn

- What is a business continuity plan?
- What is business resilience?
- What is Compliance Management?
- What is GRC?
- What is operational resilience?
- What is operational risk management?
- What is ransomware?
- What is third party risk management (TPRM)?

### Get started

- Work with an implementation specialist to achieve your desired business outcomes. To learn more, visit the Customer Success Center.
- Take a Governance, Risk, and Compliance course to build expertise and realize ROI faster. To sign up, see ServiceNow training and certification.

### Applications and features

- Audit Management
- Business Continuity Management
- Continuous Authorization & Monitoring
- Operational Resilience
- Policy and Compliance Management
- Privacy Management
- Regulatory Change Management
- Risk Management
- Third-party Risk Management
- GRC and the ServiceNow Store
- Common GRC Features

## GRC and the ServiceNow Store

All GRC applications are available from the ServiceNow Store, allowing you to obtain new and updated features more rapidly. Before you can use any GRC applications, you must verify that you have entitlement to them (that is, you have valid licenses to use them). Then, you can download them from the ServiceNow Store and activate them.

### Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

The list of GRC applications available for download includes:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Audit Management (and supported integrations)
- Business Continuity Management
- Operational Resilience
- Policy and Compliance Management (and supported integrations)
- Regulatory Change Management
- Risk Management (and supported integrations)
- Vendor Risk Management (and supported integrations)

Watch this five-minute video to learn about downloading Security Operations and GRC applications from the ServiceNow Store. This 5-minute video describes how to download Security Operations and GRC applications from the ServiceNow Store

The process you use to obtain GRC products depends on whether you are downloading a product for the first time, updating a product that you previously downloaded from the ServiceNow Store, or upgrading from one family release to the next one.

## Download a GRC application from the ServiceNow Store for the first time

Downloading an application from the ServiceNow Store for the first time involves several easy steps. Some steps are performed on the ServiceNow Store and some in your Now Platform instance.

**Before you begin**
Role required: admin

**About this task**
The ServiceNow Store allows you to download core products and applications. A product contains one or more applications that are licensed as a group. For example, GRC is a product. The process involves these steps:

- In the ServiceNow Store, you must ensure that you have entitlements (or licenses) to the application and its dependent applications.
- Activate the application and run it on your instance.

Starting in Orlando, dependency plugins are automatically installed when you activate these GRC core applications:

- Audit Management
- Policy and Compliance Management
- Risk Management

For example, when you activate the Risk Management application, the Risk Management Dependencies plugin is also activated.

**Important:** Vendor Risk Management, you must first activate the Vendor Risk Management Dependencies plugin before activating the Vendor Risk Management application. For more information, see Activate an entitled GRC ServiceNow Store application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Get entitlement for a GRC product or application

The first step in installing an application is to verify that the application or the product and its associated applications have valid ServiceNow entitlements.

### Before you begin

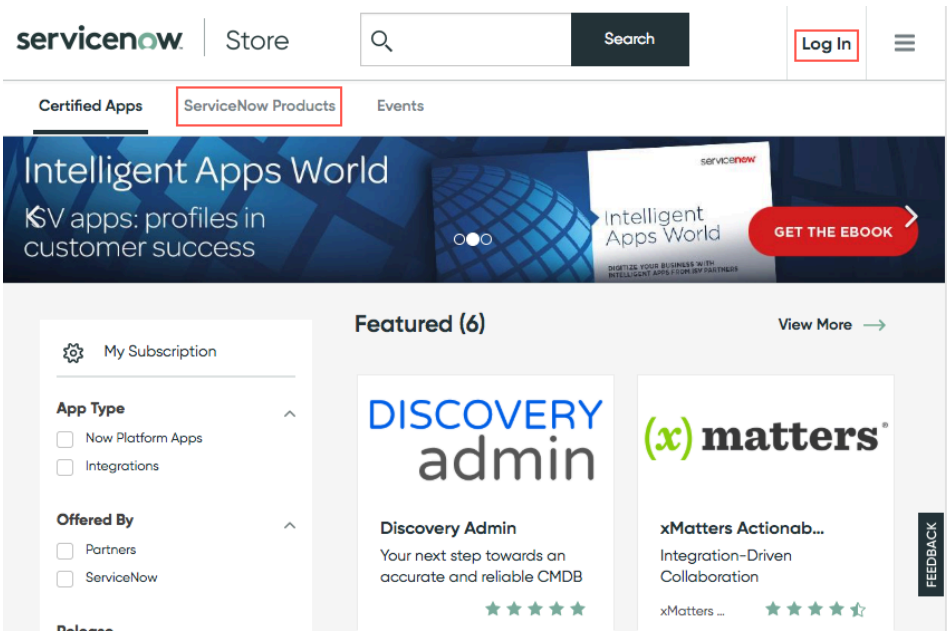
Role required: admin

Individuals performing entitlement must have a Now Support account and have permission to request applications for the instances under consideration.

**Note:** This process applies only to applications downloaded to production instances. If you are downloading applications to sub-production or development instances, it is not necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

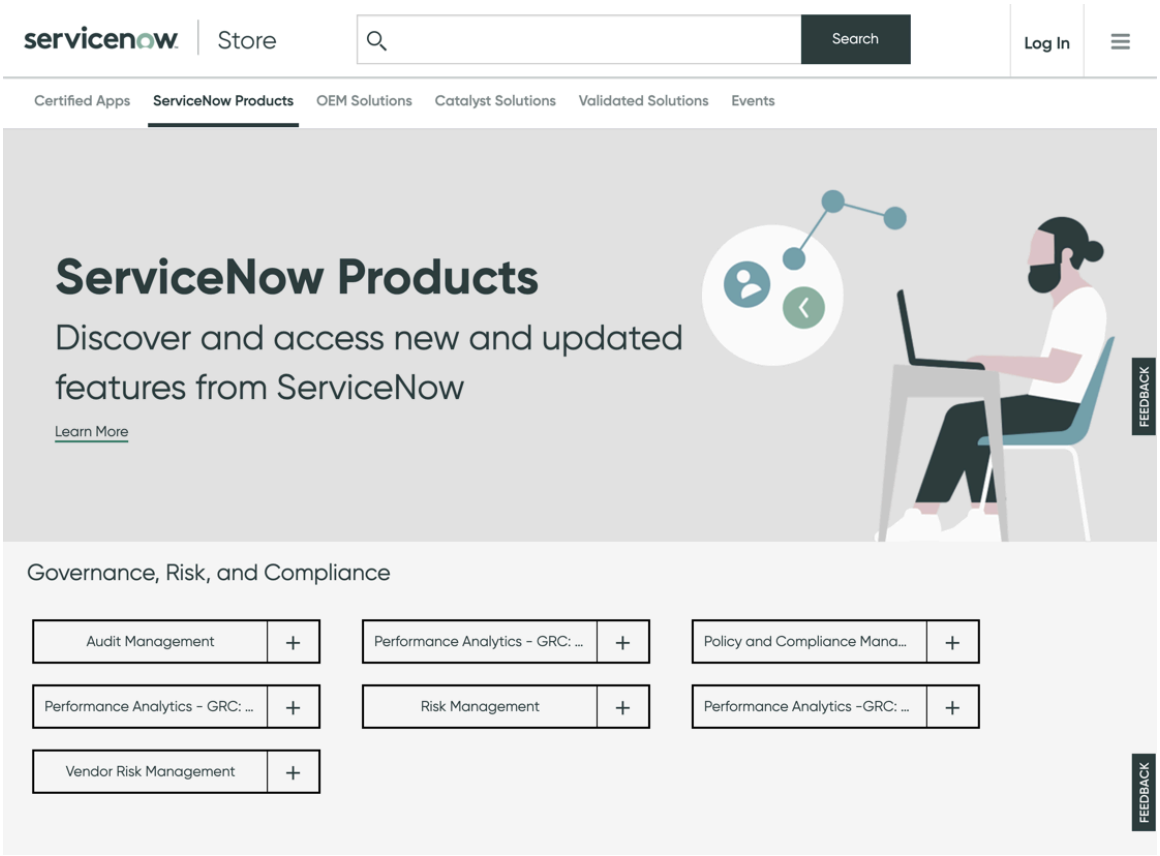
### Procedure

1. Navigate to the ServiceNow Store.



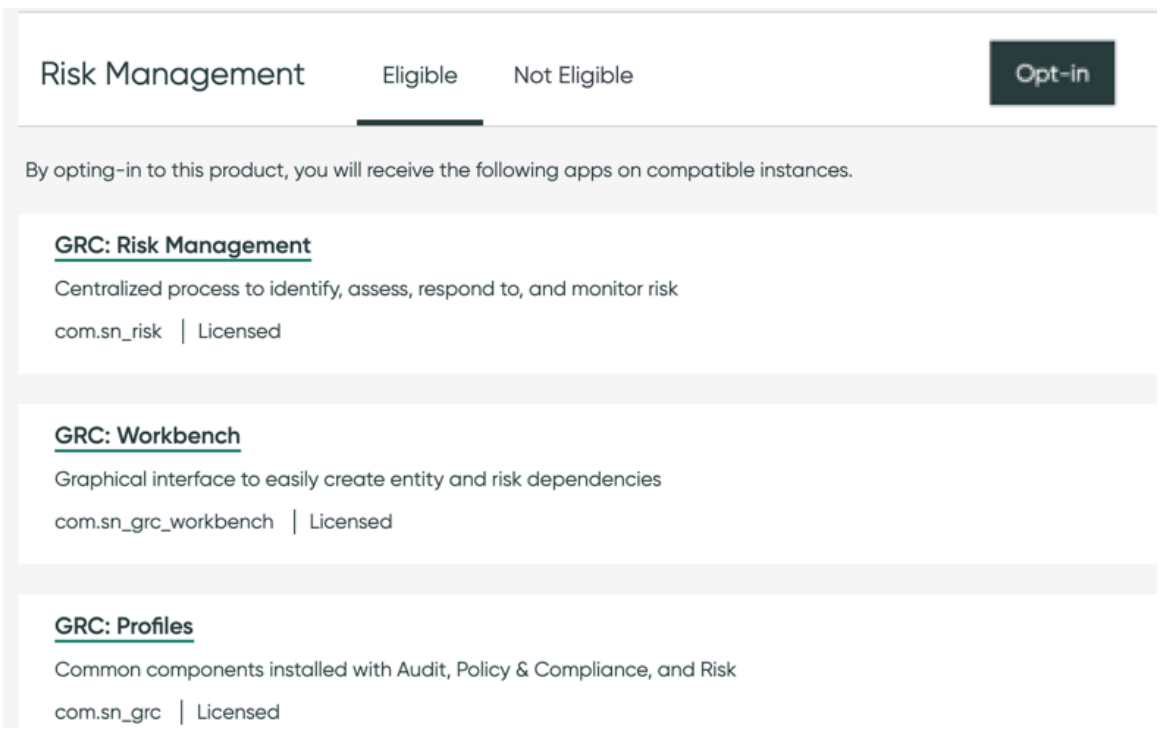

2. Click **Login** and log in using your HI credentials.
3. Click the **ServiceNow Products** tab to view all available ServiceNow products. Integrations and other types of content are shown on the **Certified Apps** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



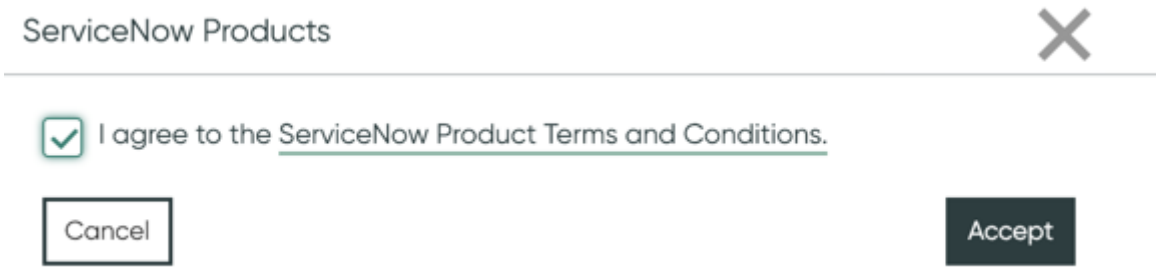

**Note:** For the sake of this example, assume you are acquiring entitlement for the Risk Management product.

4. Click the product name of the product you are getting entitlement to.
   All applications associated with the product you are entitling are listed. When you have obtained entitlement to the core product, the applications listed under it are also entitled.

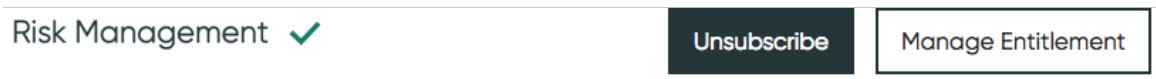



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Opt-in** to verify that you have entitlement to the product and the applications listed. You are prompted to read and accept the ServiceNow terms and conditions.

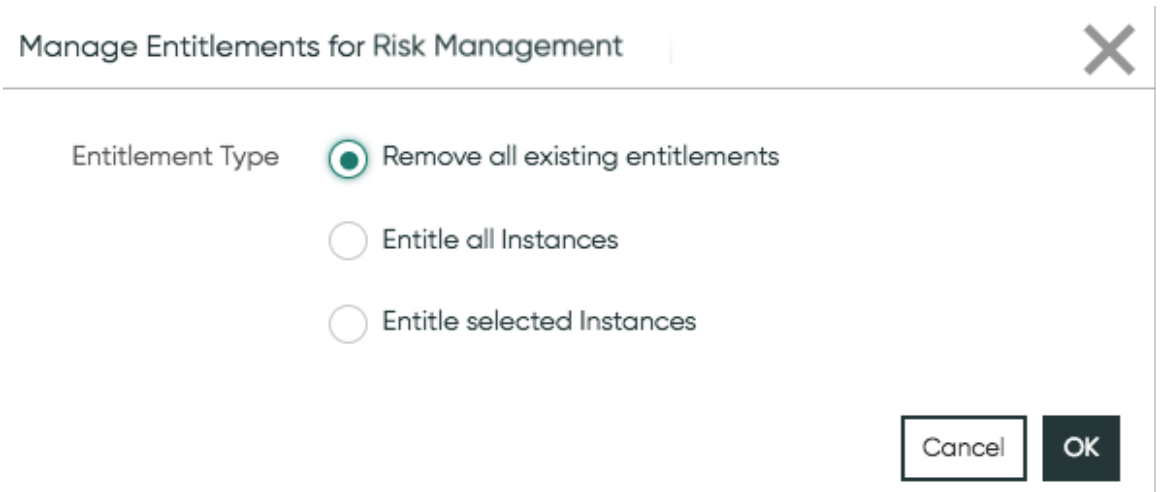



6. Select the check box and click **Accept**.
7. Notice that a check mark appears next to the product name and the Manage Entitlements button appears.




The check mark indicates that you have subscribed to the product and its associated applications. It is time to manage your entitlements. This is a one-time process for this product and any other products you want to install in the future.

8. Optional: Click **Manage Entitlements** to change the instances affected by the applications to which you are entitled.




9. After you have agreed to the ServiceNow Terms and Conditions and managed entitlements, you can entitle other products by clicking the plus sign (+) next to the product name.

**Note:** You are now ready to activate the product.

## Activate an entitled GRC ServiceNow Store application

After an application has been given entitlement, you can activate it. This process applies to applications downloaded to sub-production instances.

**Before you begin**
Role required: admin

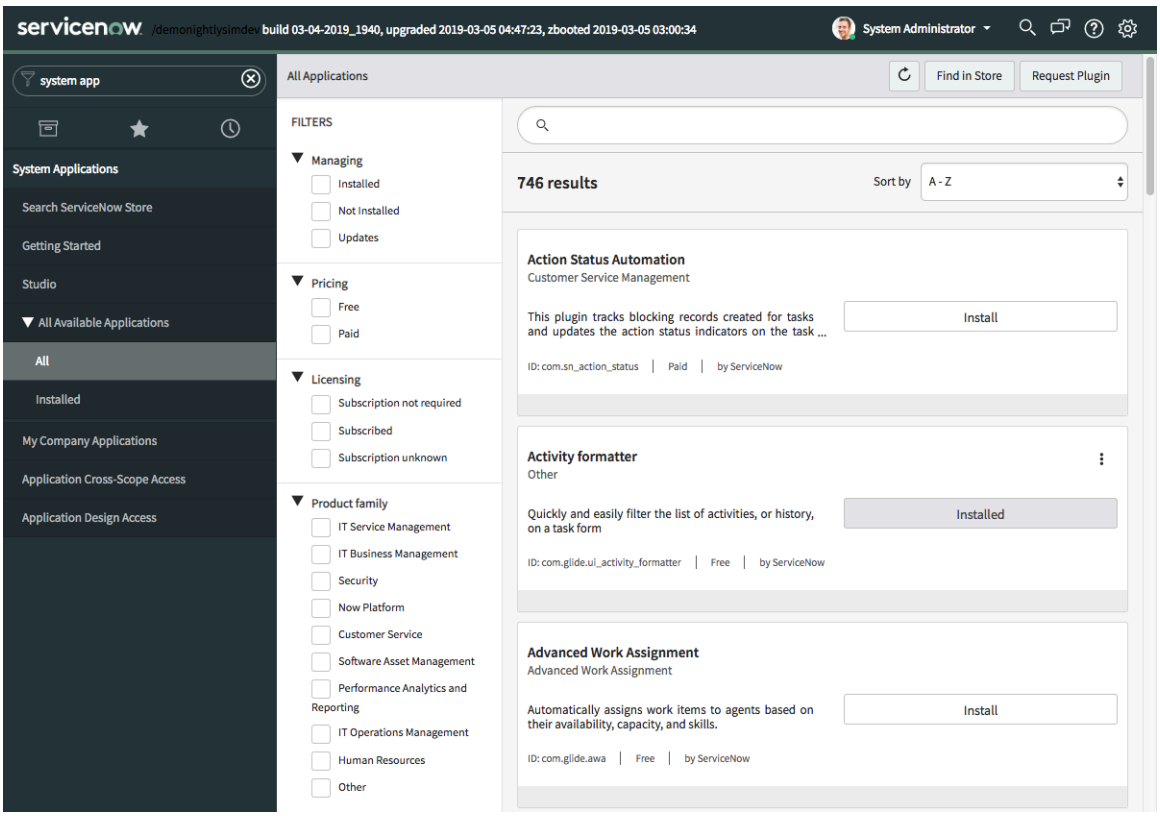
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

IntegrationHub entitlements included in Compliance Workspace are solely restricted to use by Policy authoring – integration with O365. All other use requires the applicable purchase of additional IntegrationHub entitlement. For Policy authoring – integration with O365, you require the following spokes:

- Microsoft OneDrive Spoke version 2.1.1
- Microsoft OneDrive Spoke for Document Service Framework version 1.0.5

### Procedure

**1.** Navigate to **System Applications** > **All Available Applications** > **All**.



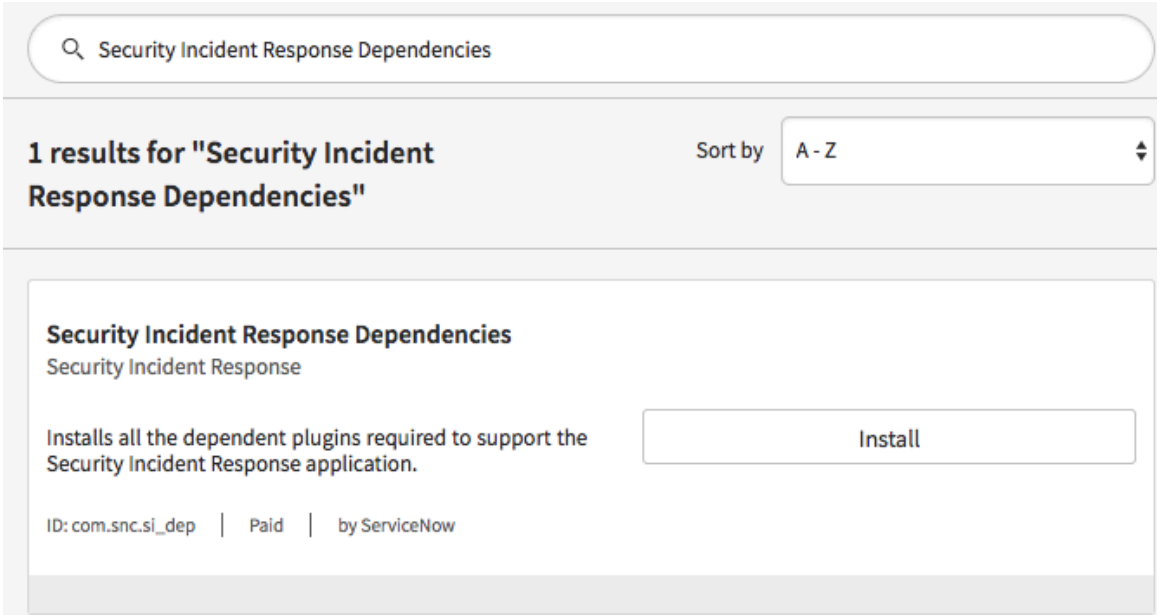

**Note:**

Starting with Orlando, dependency plugins are automatically activated when you activate a core application. For example, when you activate the Audit Management application, the Audit Management Dependencies plugin is also activated.

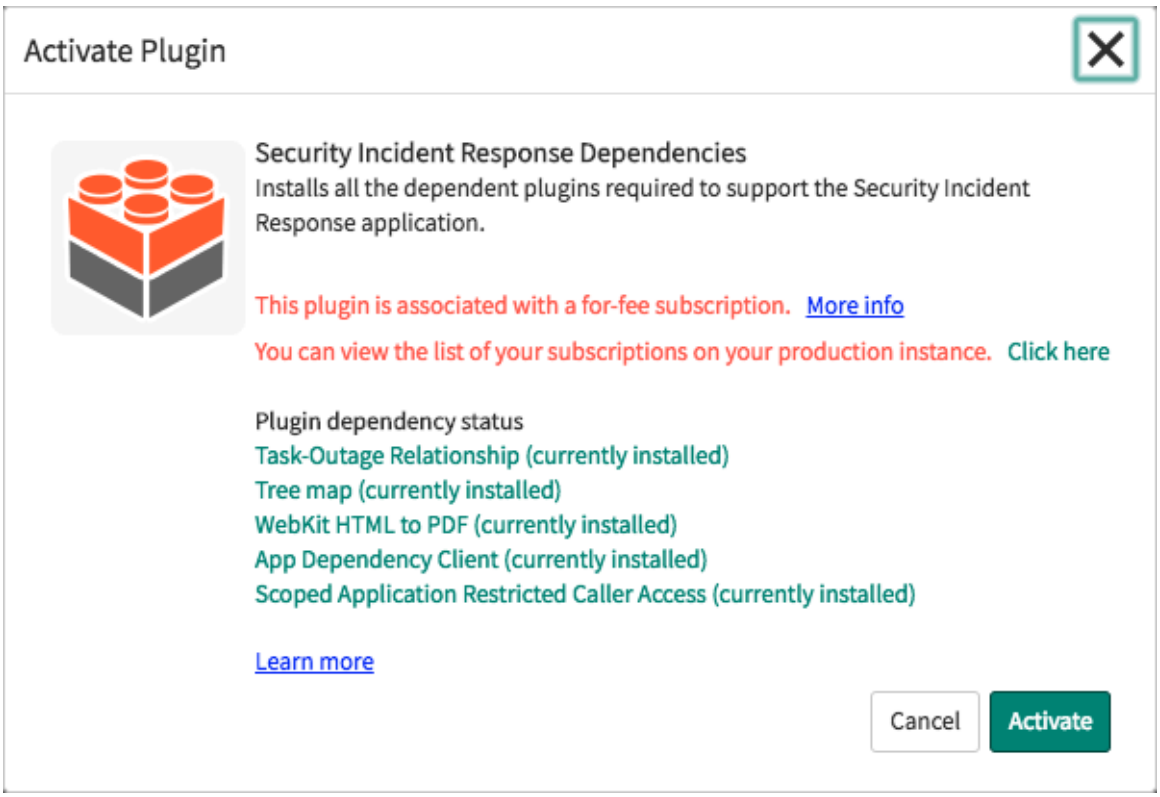
**Important**The information in the previous Note does not apply to the Vendor Risk Management application. If you are activating Vendor Risk Management, proceed with the next step. If you are activating any of the other GRC applications, steps 2 through 5 are optional.

**2.** Search for the dependencies plugin for the application you want to activate.
For example, if you are activating Security Incident Response, locate the Security Incident Response Dependencies plugin.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. Click **Install**.
   The Activate Plugin dialog box appears.




4. In the Activate Plugin dialog box, click **Activate**.
5. When the activation is complete, click **Close & Reload Form**.
6. Locate the core product you are activating.
7. If you want to load demo data, click the **Load demo data** check box.
8. Click **Install**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Your application is automatically installed on your instance.

**Note:** If you do not select the **Load demo data** check box, demo data is not available to install from the **Application Manager** later. For information on how to install or reinstall demo data after the initial installation, see the Work around to install demo data if application is already installed [KB0722909] article in the HI Knowledge Base.

## Install GRC content packs and integrations

All ServiceNow integrations are available on the ServiceNow Store. Core applications, such as Policy and Compliance Management, are visible in the **ServiceNow Products** tab on the store. Content pack and integration add-ons are visible in the **Certified Apps** tab.

### Before you begin

Role required: admin
Sore installation requires a Now Support account and have permission to request applications for the instances under consideration.

### Procedure

1. Navigate to **System Applications** > **All Available Applications** > **All**.
2. Locate the application you want to install and click **Install**.
   - If you are installing the app to a sub-production instance, the application installs on the instance.
   - If you are installing the app to a production instance, and you have a valid license (that is, you have entitlement to the application), the application installs on the instance.
   - If you are installing the app to a production instance, and you do not have a valid license, a message is shown. Perform the following steps.

**a.** Click **Find in Store** to open the ServiceNow Store.

**b.** Locate the application and click its tile.

**c.** Click **Get** and enter your Now Support login credentials.

**d.** Click **Request Install**.

**Note:** For store applications developed by ServiceNow, the **Get** button is shown.

**e.** Click **Request**.
Enter the instance name and a reason for the request, then click **Request**. You are sent an email with detailed installation instructions.

**f.** Navigate to **System Applications** > **All Available Applications** > **All**.
A list of applications available for installation is displayed.

**g.** Click **Install**.
Locate the application, select it, and click **Install**. Your application is automatically installed on your instance.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Update a GRC application previously downloaded from the ServiceNow Store

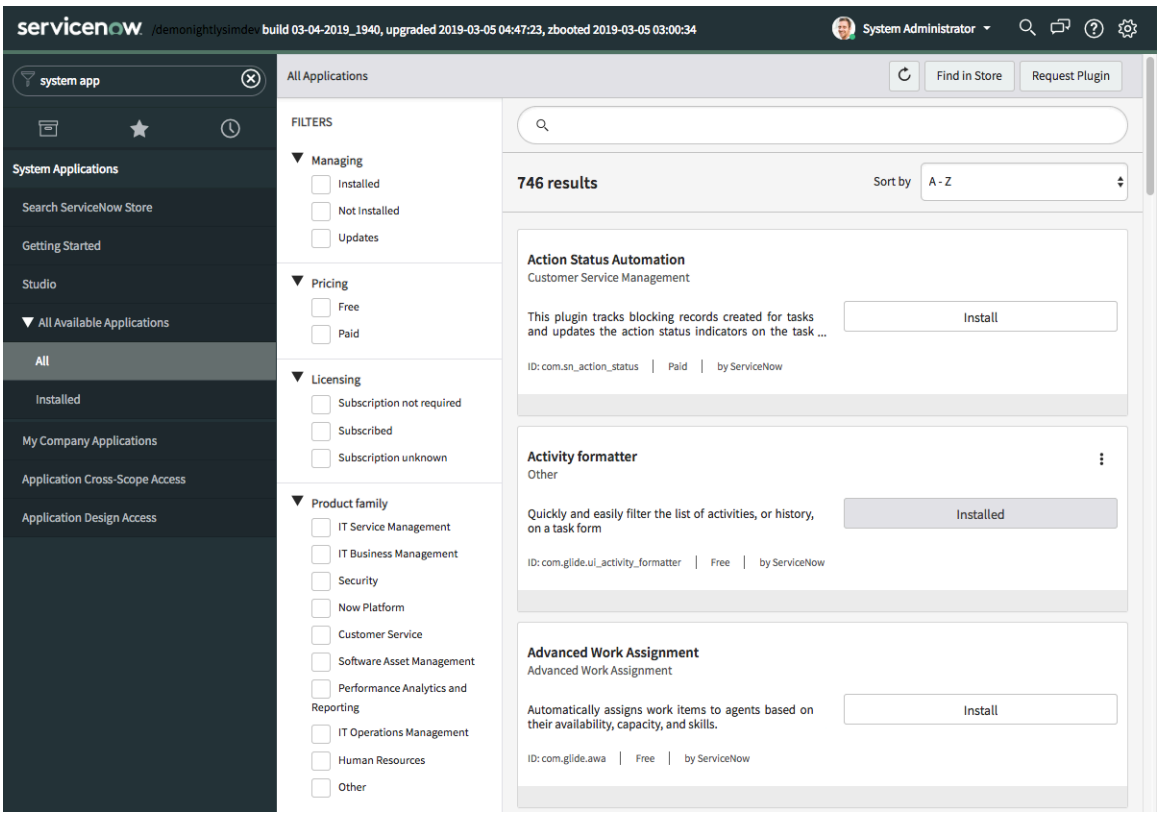
If you have previously downloaded an application from the ServiceNow Store and a new version is available, you can update it in your instance.

### Before you begin

Role required: admin

### Procedure

1. Navigate to **System Applications** > **All Available Applications** > **All**.




2. Search for the application you want to update.
3. Select the version you want to update to and click **Update**.
   Your application is automatically updated on your instance.

## Upgrade your instance to the next GRC family release

If you are currently running a family release (London for example) and want to upgrade to the next release, it is not necessary to acquire the applications from the ServiceNow Store. The application is automatically updated when the platform is updated to the minimum required version.

# Audit Management

The ServiceNow® Audit Management application involves a set of activities related to planning audit engagements, executing engagements, and reporting findings to the audit committee and executive board. Engagement reporting assures key stakeholders that the organization's risk and compliance management strategy is effective.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Audit workspace

As of version 13.0.2, there are two interfaces available for Audit Management users. They are the Classic model and Audit workspace. The Audit workspace offers a single-pane view for the audit supervisors and auditors to view the overall audit timeline and status, track budget and resources for engagement, and monitor control tests and audit task progress. For more information on the new workspace, see Risk workspace.

### Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

The GRC: Audit Management product allows you to schedule internal audits, conduct resource planning, and scope engagements. You can also conduct audit activities, review continuous monitoring results, and report findings.

| Explore | Set up | Administer |
| --- | --- | --- |
| | Activate Audit Management | Engagement Overview |
| **Use**<br>• Governance, Risk, and Compliance entity scoping<br>• Use the Audit Engagement Workbench to visually manage engagements<br>• Manage test templates and test plans | **Develop**<br>•<br>• Developer documenta-<br>• Components installed with Audit Management | **Troubleshoot and get help**<br>• Ask or answer questions in<br>• Search the Known Error Por-<br>• Contact Customer Service |

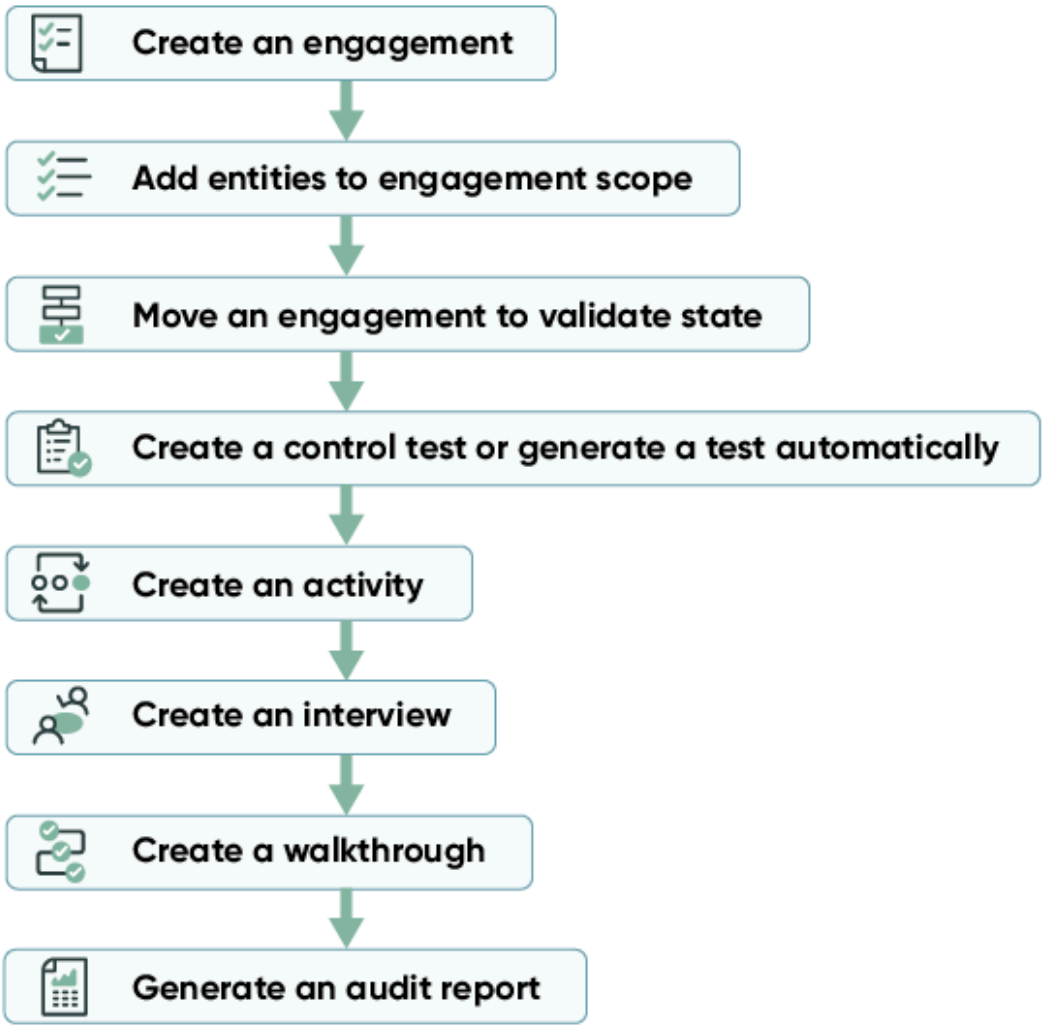
## GRC Audit Management implementation

Use the steps in the GRC Audit Management application checklist to download the Audit Management from the ServiceNow Store, and get it ready for operation. Mandatory and optional setup steps, as well as an implementation checklist, are provided to simplify the setup.

The flow of mandatory steps in the checklist are as follows:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Audit Management implementation steps**




## Setup checklist for the GRC Audit Management application

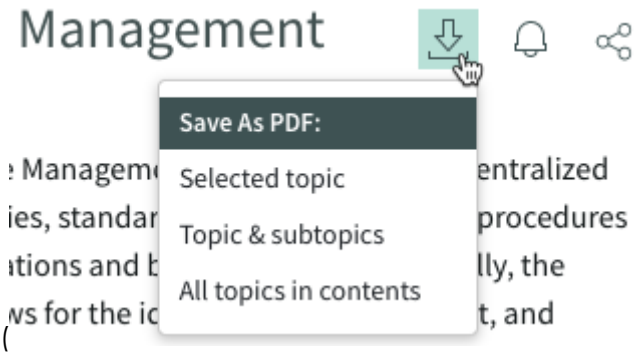
This checklist includes the setup tasks that you are required to complete in your Now Platform® instance. When you have completed these tasks, the base system is ready for operation. Optional setup procedures are also included to enhance Audit Management functionality.

**Before you begin**
Role required: admin

Consider creating and printing a PDF of this checklist topic. You can then check off tasks as you complete them.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To generate a PDF, click the save as PDF icon




( ) at the top of the topic.

**Procedure**

Click the **Selected topic**.

**Audit Management application checklist**

| Item | Description |
|---|---|
| ☐ | As an audit administrator or audit manager, create engagements to manage audit information and include entities, controls, and control tests that are relevant to the audit. For details, see Create an engagement. |
| ☐ | As an audit administrator or audit manager, after you have created engagements, define which entities are scoped in the audit engagement. For details, see Add entities to an engagement scope. |
| ☐ | After defining a control, audit managers create control tests that run periodically and provide documented evidence of whether the associated control is operating correctly. For details, see Create a control test from an engagement. You can also generate control tests automatically. For details, see Automatically generate control tests from an engagement |
| ☐ | After defining a control, audit managers create activities that explore and provide documented evidence of whether the associated control is operating correctly. For details, see Create an audit task activity. |
| ☐ | After defining a control, audit managers create interviews with control owners to discuss and provide documented evidence of whether the associated control is operating correctly. For details, see Create an interview |
| ☐ | After defining a control, audit managers create walkthroughs that will be conducted to observe and provide documented evidence of whether the associated control is operating correctly. For details, see Create a walkthrough. |
| ☐ | As an audit manager, generate an audit report that summarizes the findings of an engagement so report findings can be communicated to executives. For details, see Generate an audit report from an engagement |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Download Audit Management

Before you run GRC: Audit Management (com.sn_audit) in your instance, you must download it from the ServiceNow Store.

### Before you begin

Role required: admin

### Procedure

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

#### Quick start tests for Audit Management

Validate that GRC: Audit Management still works after you make any configuration change such as apply an upgrade or develop an application. Copy and customize these quick start tests to pass when using your instance-specific data.

## GRC Audit Management

GRC: Audit Management quick start tests require activating the GRC: Audit Management plugin (com.sn_audit) and loading the demo data.

**GRC: Audit Management test suite**

| Test | Description | Release version |
|---|---|---|
| GRC: Create Audit Engagement and Generate Audit Task | Validates audit engagement creation and associates entities to generate controls and test plans. Generates audit task which is associated to a test plan. | Paris |
| GRC: Create and process a milestone | Create a milestone in an engagement, notice that the due date cannot be in past and the completion date cannot be in future and for a milestone in open state the percent complete is 0 which changes in accordance with the milestone state change. | Paris |
| GRC: Cost and Resource plan rollup | Create an audit plan and associate an engagement to it, on adding cost plan and resource plan to this engagement, notice that these costs are rolled up to the plan. Any edits to these costs in engagement reflects in the plan. | Paris |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**GRC: Audit Management test suite (continued)**

| Test | Description | Release version |
|---|---|---|
| GRC: Create Engagement Project Manual and automatic | On an engagement in the validate state, once the Enable advanced planning ui-action is performed notice an engagement project gets created and when the state of an engagement associated to an audit plan having "Advanced planning capabilities" is changed to validate notice that an engagement project gets created automatically. | Paris |
| GRC: Auditable Unit with Detailed Risk Assessment | Create an Auditable unit with method as "Detailed Risk Assessment" and request for Assessing the Risk Assessment by adding the Assessor once the assessor responds and Marks Assessment as Complete after performing the control assessment and residual assessment, the risk assessment fields should be auto updated. | Paris |

To learn more about Audit Management, see Audit Management.

Related topics

Quick start tests

### Components installed with Audit Management

Activating the GRC: Audit Management (com.sn_audit) plugin adds or modifies several tables, user roles, and other components.

### Properties installed with Audit Management and Advanced Audit

Properties are added with activation of GRC: Audit Management.

| Name | Description | Application |
|---|---|---|
| sn_audit.knowledge_base | Name of the knowledge base used to publish Audit reports<br>• Type: string<br>• Default value: Audit | Audit Management |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Name | Description | Application |
|---|---|---|
| sn_audit_advanced.default_adv_notification_duedate_duration | Default duration (in days) from the due date of a milestone, based on which, a notification will be sent.<br>• Type: integer<br>• Default value: 8 | GRC: Advanced Audit |
| sn_audit_advanced.role_documentation_link | Documentation link for role requirements for enabling and using advanced planning feature (with PPM integration).<br>Type: string | GRC: Advanced Audit |
| sn_audit_advanced.ppm_project_documentation_link | Documentation link for project capabilities and role requirements.<br>Type: string | GRC: Advanced Audit |
| sn_audit_advanced.rollup_documentation_link | Documentation link for expenses and resources rollup details, from project to related engagement and plan.<br>Type: string | GRC: Advanced Audit |

### Roles installed with Audit Management

Roles are added with activation of GRC: Audit Management.

| Role title [name] | Description | Contains roles |
|---|---|---|
| Audit Admin<br>[sn_audit.admin] | In addition to the inherited permissions, the audit admin can delete engagements, audit tasks, test templates, and test plans. | • sn_audit.manager<br>• sn_grc.admin |
| Audit Developer<br>[sn_audit.developer] | In addition to the inherited permissions, the audit developer can add and delete audit report templates. | • sn_audit.admin<br>• sn_grc.developer |
| External Auditor<br>[sn_audit.external_auditor] | External auditors can be assigned as auditors for an engagement and can be assigned to audit tasks. They can view closed engagements, audit tasks that are assigned to them, and closed audit tasks. If the Policy and Compliance | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role title [name] | Description | Contains roles |
|---|---|---|
| | Management plugin or Risk Management plugins are installed, they can also view published policies and all controls and risks in the **Monitor** state. | |
| Audit Manager<br><br>[sn_audit.manager] | In addition to the inherited permissions, the audit manager can create audit tasks (such as control tests, activities, walkthroughs, and interviews), engagements, test plans, test templates, issues, remediation tasks, and entities. If Advanced Core is installed, then the audit manager can also create evidence requests. | • sn_audit.user<br>• sn_grc.manager |
| Audit User<br><br>[sn_audit.user] | In addition to the inherited permissions, the audit user can be assigned audit tasks and create test templates and test plans. The audit user has read-only access to the Risk Management application and modules and the Policy and Compliance Management application and modules. | • sn_compliance.reader<br>• sn_grc.reader<br>• sn_grc.user |
| Engagement Project Manager<br><br>[sn_audit_advanced.engagement_project_manager] | The audit lead who does advanced planning and could handle plans or engagements. | • sn_audit.manager<br>• resource_manager<br>• it_project_manager |

### Tables installed with Audit Management

Tables are added with activation of GRC: Audit Management.

| Table | Description |
|---|---|
| Activity<br><br>[sn_audit_activity] | Extends Audit Task [sn_audit_task] and stores audit activities |
| Audit Task<br><br>[sn_audit_task] | Extends Planned Task [planned_task] and is a generic table for all tasks associated with an audit |
| Base Audit Test<br><br>[sn_audit_base_test] | Base table for Test Templates and Test Plans |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Table | Description |
| --- | --- |
| Control Test<br><br>[sn_audit_control_test] | Extends Audit Task [sn_audit_task] and stores control tests |
| Control to Engagement<br><br>[sn_audit_m2m_control_engagement] | Stores many-to-many relationships between controls and engagements |
| Engagement<br><br>[sn_audit_engagement] | Extends Planned Task [planned_task] and stores engagements |
| Interview<br><br>[sn_audit_interview] | Extends Audit Task [sn_audit_task] and stores interviews |
| Entity to Engagement<br><br>[sn_audit_m2m_profile_engagement] | Stores many-to-many relationships between entities and engagements |
| Risk to Engagement<br><br>[sn_audit_m2m_risk_engagement] | Stores many-to-many relationships between risks and engagements |
| Test Plan<br><br>[sn_audit_test_plan] | Extends Base Audit Test [sn_audit_base_test] and stores test plans |
| Test plan to Engagement<br><br>[sn_audit_m2m_test_plan_engagement] | Stores many-to-many relationships between test plans and engagements |
| Test Template<br><br>[sn_audit_test_template] | Extends Base Audit Test [sn_audit_base_test] and stores test templates |
| Walkthrough<br><br>[sn_audit_walkthrough] | Extends Audit Task [sn_audit_task] and stores walkthroughs |
| Audit Report Template<br><br>[sn_audit_report_template] | Stores the defined xml, html, or script-based audit report templates |
| Assessment procedures<br><br>[sn_audit_asmnt_procedure_control_test] | Stores the assessment objectives of control tests. Identifier and assessment objectives field values are copied over from the Assessment procedure plan table. |
| Assessment procedure plan<br><br>[sn_audit_asmnt_procedure_test_plan] | Generated for the test plan. Changes made to the test plan are reflected in the control test table [sn_audit_asmnt_procedure_control_test] |
| Assessment procedure templates<br><br>[sn_audit_asmnt_procedure] | Stores the assessment objectives |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Table | Description |
| --- | --- |
| Test template to Assessment procedure<br>[sn_audit_m2m_test_temp_asmnt_procedure] | Stores many-to-many relationships between test template and assessment procedure |

**Note:** All additional tables installed by the dependent plugins are also needed for GRC: Audit Management.

### Tables installed with Advanced Audit

Tables are added with activation of GRC: Advanced Audit

| Table | Description |
| --- | --- |
| Audit Task to Milestone<br>sn_audit_advanced_m2m_audit_task_milestone | Stores many-to-many relationships between audit tasks and milestones. |
| Auditable Unit<br>sn_audit_advanced_auditable_unit | Stores auditable units. |
| Auditable Unit To Authority Document<br>sn_audit_advanced_m2m_unit_authority_document | Stores many-to-many relationships between auditable units and authority documents. |
| Auditable Unit To Business Application<br>sn_audit_advanced_m2m_unit_business_application | Stores many-to-many relationships between auditable units and business applications. |
| Auditable Unit To Business Process<br>sn_audit_advanced_m2m_unit_business_process | Stores many-to-many relationships between auditable units and business processes. |
| Auditable Unit To Business Unit<br>sn_audit_advanced_m2m_unit_business_unit | Stores many-to-many relationships between auditable units and business units. |
| Auditable Unit To Department<br>sn_audit_advanced_m2m_unit_cmn_department | Stores many-to-many relationships between auditable units and departments. |
| Auditable Unit To Location<br>sn_audit_advanced_m2m_unit_location | Stores many-to-many relationships between auditable units and locations. |
| Auditable Unit To Policy<br>sn_audit_advanced_m2m_unit_policy | Stores many-to-many relationships between auditable units and policies. |
| Auditable Unit To Product<br>sn_audit_advanced_m2m_unit_product_model | Stores many-to-many relationships between auditable units and products. |
| Auditable Unit To Vendor<br>sn_audit_advanced_m2m_unit_vendor | Stores many-to-many relationships between auditable units and vendors. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Table | Description |
|---|---|
| Engagement Project<br><br>sn_audit_advanced_engagement_project | Extends Project table and stores engagement projects for engagements. |
| Milestone<br><br>sn_audit_advanced_milestone | Extends Planned Task table and stores milestones. |
| Observation<br><br>sn_audit_advanced_observation | Extends Triage table and stores observations. |
| Plan<br><br>sn_audit_advanced_plan | Extends Planned Task table and stores plans. |

**Note:** All additional tables installed by the dependent plugins are also needed for GRC: Audit Management.

## Setup checklist for the GRC Advanced Audit application

Complete the checklist that includes the setup tasks required to complete in your Now Platform® instance. When you have completed these tasks, the base system is ready for operation.

### Before you begin

Role required: admin

Consider creating and printing a PDF of this checklist topic. You can then check off tasks as you complete them.

### Procedure

1. To generate a PDF, click the save as PDF icon ( ) at the top of the topic.
2. Click the **Selected topic**.

#### Audit Management application checklist

| Item | Description |
|---|---|
| ☐ | As an audit manager, and IT project manager, create an audit plan to manage different types of audits in a periodic manner and group engagements in a logical manner. For details see, Create an audit plan |
| ☐ | As an audit user or an audit manager, create auditable units with entities such as business units, departments, vendors, products, business processes, business applications, locations, authority documents, and policies to perform risk assessments on the auditable units. For details, see Create an auditable unit |
| ☐ | As an audit manager, use the advanced planning capabilities to create an engagement that automatically creates an engagement project. For details, see Create an engagement with advanced planning |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Item | Description |
|---|---|
| ☐ | As an audit manager, create milestones that can be used to track the progress of an engagement.<br><br>After you create milestones for an engagement, you can also add audit tasks to the milestone and track those tasks as milestones. For details see, Create an engagement milestone |
| ☐ | As a resource user, you can create a resource plan from the Resource Management application for any task such as demand, project, project task, incident, problem, or change. You can edit and adjust the plan until you submit it for approval. For details see, Create a resource plan |
| ☐ | As an IT project manager, create a cost plan to specify the unit cost of a cost type for a fiscal period. Project cost plans capture the costs of projects. For details see, Create a cost plan |
| ☐ | Audit observations are the results of an audit. As an important part of the audit report, audit observations represent the results of reviews, analysis, interviews, and discussions. For details see, Audit observations |
| ☐ | As an audit user, request evidence. Evidence request is used by audit and compliance teams for requesting supporting documents during an audit. Auditors and compliance teams require these documents from the first line of defense. For details see, Request evidence for audit |

## Audit Management workspace

Audit workspace is a single-pane view for audit supervisor and auditor to view the overall audit timeline and status, track budget and resources for engagements, trace high priority observations and issues, and monitor ongoing control testing and audit task progress.

### Highlights of the new Audit Workspace

The workspace provides a new user experience.

- Default home page for the audit supervisor and auditor displays actionable insights and quick links.
- Organized navigation menu that lists the modules based on each user's needs.
- Re-imagined page layout with improved experience for practitioners, business users, and executives.
- Record pages that provide holistic view and actionable insights specific to what is being viewed.
- 360° view to consider scores and ratings, and visualize data relationship across the enterprise for a record.

### Audit supervisor view

An audit supervisor can use the workspace to:

- define plans and engagements
- assign budget and resource to engagements
- track the progress of engagements

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Auditor view

An auditor using the workspace can:

- test effectiveness of controls
- request evidence
- create observations
- complete all audit activities

## Audit Workspace for the Audit supervisor

An audit supervisor organizes and manages internal audits according to plans.

## Overview of audit supervisor workspace

Audit workspace provides a personalized experience for audit supervisors to manage their work better. There are four main sections that help in accomplishing their audit tasks better.

Overview

Provides the audit timeline and overview.

Tracking

Provides a summary of audit tasks, issues, observations.

Open audits

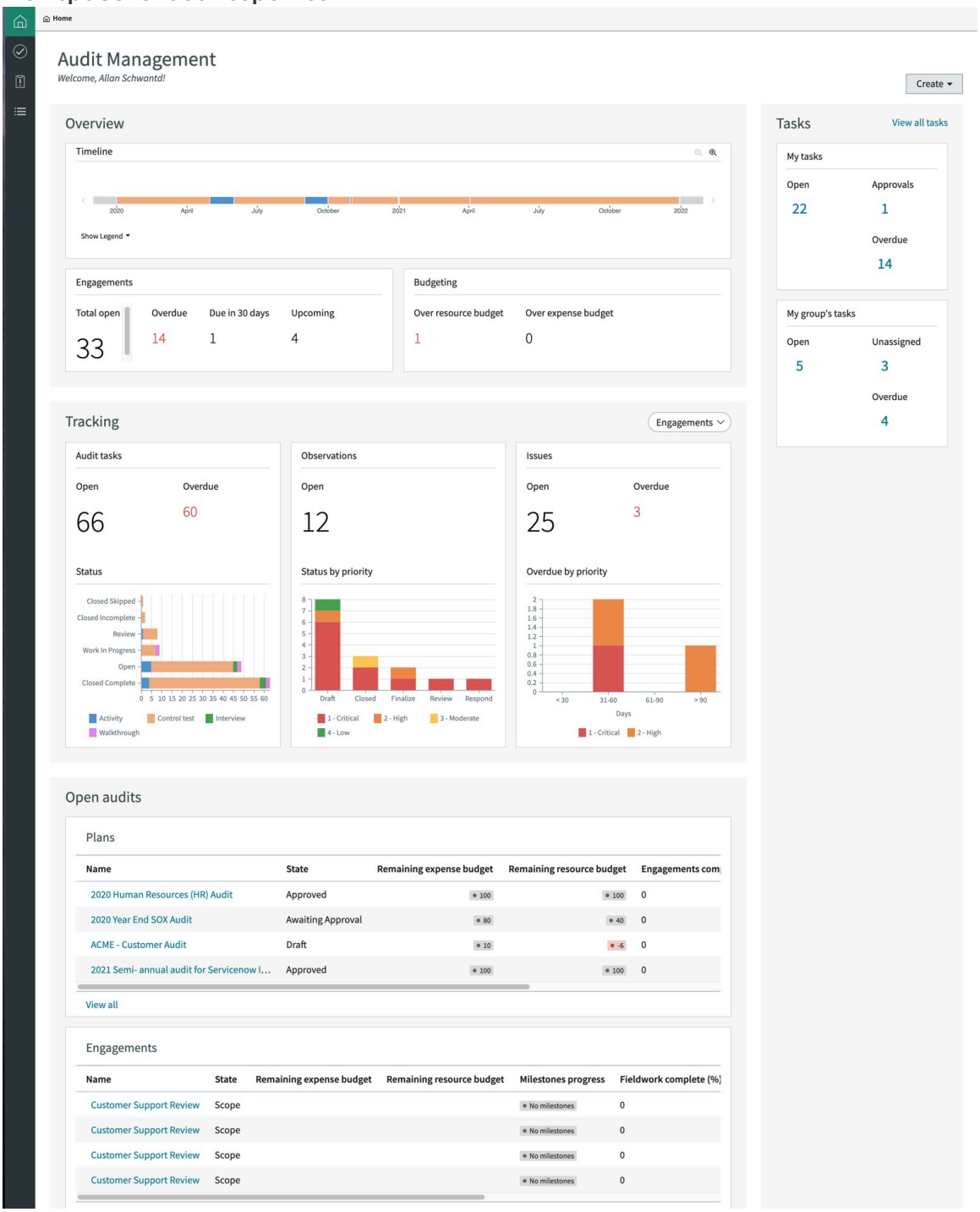
Provides details of open plan and engagement details.

Tasks

Provides a summary of the logged in user's tasks and the group's tasks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

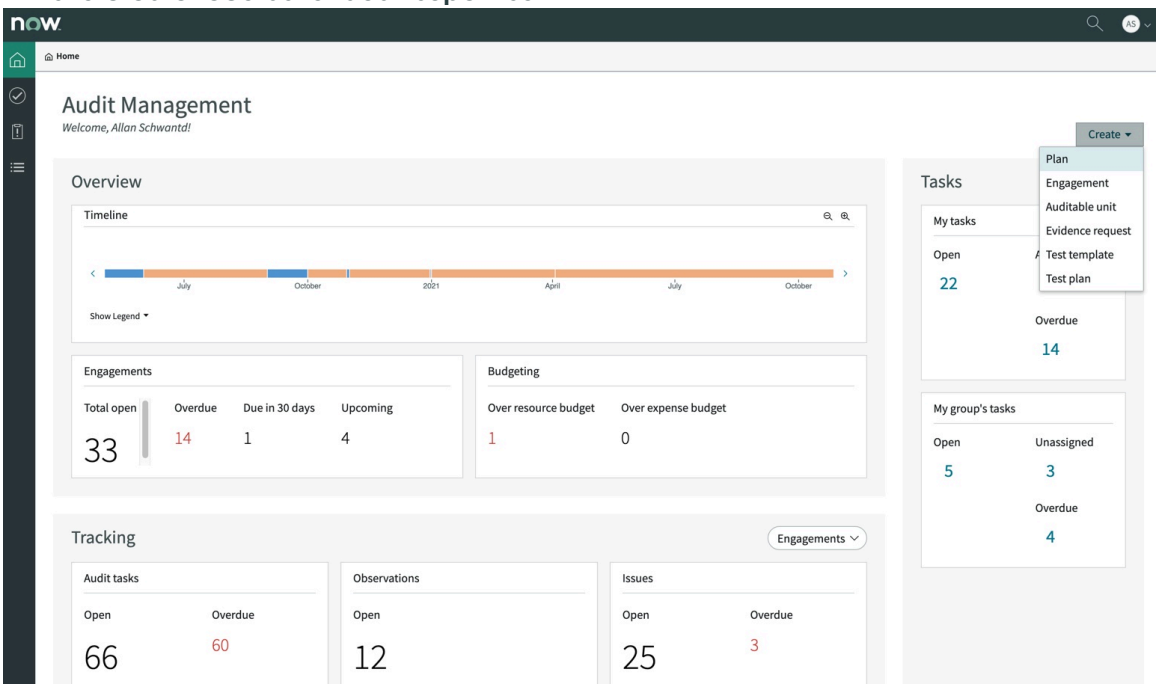
## Workspace for audit supervisor




The audit supervisor workspace also provides quick links to create new records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Links to create records for audit supervisor




The responsibilities of audit supervisors include overseeing the process of audits, making recommendations on policies, and ensuring that the organization fulfills international and governmental obligations of compliance.

## Tasks of an audit supervisor

The following table lists the key tasks that you perform in your role as an Audit supervisor.

### Tasks of an Audit supervisor

| Activity | Task |
|---|---|
| Plan and schedule audit programs and send plans for approval. | Create a plan |
| Approve an plan. | Approve a plan |
| Create audit engagements and monitor the progress. | Create an audit engagement |
| Perform risk assessments and scope auditable units and entities based on the risk rating. | Create auditable units and scope entities at risk |
| Create test plans to document control testing procedure. Coordinate walkthroughs and interviews for assessing internal control processes. | • Create a test template<br>• Create a test plan |
| Review audit observations, issues and follow up on them. | • Create issues for the engagement<br>• Create observations for the engagement |
| Review and approve audit engagements. | Approve or reject an engagement |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tasks of an Audit supervisor (continued)**

| Activity | Task |
|---|---|
| Developing recommendations and reports based on audits and presenting these ideas to senior management. | Generating report for an engagement |

### Create a test template in Audit Workspace

Create a test template and use it to create test plans applying much of the same testing criteria.

## Before you begin

Role required: sn_audit.manager, sn_audit_ws.supervisor, sn_audit.user, sn_audit_ws.auditor

## Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Click **Create** and select **Test template** from the **Home** page.
   You can also create a test template by navigating to the Audit workspace List page.
   a. Click the lists icon (  ).
   b. Click **Test templates** in the Execution list.
   c. Click **New**.
3. On the form, fill in the fields.

**Create New Test template form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the test template. |
| Control objective | Objective that acts as a guidance for the control test. |
| Duration | Duration of the test in days, hours, minutes, and seconds. |
| Design test | |
| Design expectations | Basic requirement that should be met for a control to be effective. |
| Design assessment procedures | Procedure or steps to be followed to conclude whether the design of the control is effective to achieve the control objective or not. This is based on the design expectation. |
| Operational test | |
| Operational expectations | Expectations that should be met to ensure that the control is operating effectively to achieve the control objective. |
| Operational assessment procedures | Detailed steps, to carry out the operational expectations, which need to be performed |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | to conclude that the control is operating successfully. |

4. Click **Save**.
5. To visually explore the relationships between the different types of critical audit data that affect your business, click **360° view** button.
6. To update all associated test plan with the content of the test template that you created, click **Update all** button.
7. To create test plans for all controls related to the control objective, as in the test template, if the test plan does not exist already, then click **Create test plans for all controls** button.

### Create a test plan in Audit Workspace

Create a test plan to document the control testing procedure. You can create a test plan from scratch or based on a test template to describe how a feature is to be tested.

## Before you begin

Role required: sn_audit.manager, sn_audit_ws.supervisor, sn_audit_ws.auditor, sn_audit.user

## Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Click **Create** and select **Test plan** from the **Home** page.
   You can also create a test plan by navigating to the Audit workspace List page.
   a. Click the lists icon ( ).
   b. Click **Test plans** in the Execution list.
   c. Click **New**.

   You can also create a test plan from an engagement that is in **Validate** or **Fieldwork** state by selecting the test plan and clicking the **Generate Control Tests** button in the Test plans related list.
3. To change the content of the test plan to the content in the test template, click **Revert to template** button.
4. On the form, fill in the fields.

### Create New Test plan form

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the test plan. |
| Control | The control that this test plan covers. |
| Entity | Entity is auto-populated based on the value selected in the **Control** field. |
| Test template | Related test template.<br><br>If you select a test template, all the fields in the **Design test** and **Operational test** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | sections are populated with the test template values. |
| Duration | Expected duration of the test. |
| Design test | |
| Design expectations | Basic requirement that should be met for a control to be effective. |
| Design assessment procedures | Procedure or steps to be followed to conclude whether the design of the control is effective to achieve the control objective or not. This is based on the design expectation. |
| Operational test | |
| Operational expectations | Expectations that should be met to ensure that the control is operating effectively to achieve the control objective. |
| Operational assessment procedures | Detailed steps, to carry out the operational expectations, which need to be performed to conclude that the control is operating successfully. |

5. Click **Save**.
6. To visually explore the relationships between the different types of critical audit data that affect your business, click **360° view** button.

### Create a plan in the Audit Workspace

Create a plan to manage different types of audits in a periodic manner and group engagements in a logical manner.

## Before you begin

Activate the Advanced Audit plugin (com.sn_audit_advanced).

Role required: sn_audit_ws.supervisor or sn_audit.manager

## About this task

When an audit plan is created and engagements are added to the plan, the plan is sent to the approver for approval.

## Procedure

1. Navigate to **All** > **Audit** > **Audit workspace** > **Planning** > **All Plans**.
2. Optional:  Alternatively, navigate to **Audit** > **Audit workspace** > **Planning** > **My Plans**.
3. Select **New**.
4. On the form, fill in the fields.

#### Plan form

| Field | Description |
|---|---|
| Number | Unique number of the plan. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Name | Name of the plan. For example, Annual Audit Plan for Payroll. |
| Type | Type of the plan. The choices are:<br>◦ None<br>◦ Internal Audit Plan<br>◦ External Audit Plan<br>◦ SOX Audit<br>◦ Compliance Audit Plan<br>◦ Vendor Audit Plan<br>◦ Customer Audit Plan |
| State | State of the plan. The default state is **Draft**. |
| Substate | Substate of the plan. The value in this field changes based on the workflow. |
| Description | Brief description of the plan. |
| Objectives | Objectives of the plan. |
| Schedule | |
| Timeframe | Duration of the plan. The choices are as follows:<br>◦ Annual<br>◦ Semi-annual<br>◦ Quarter<br>◦ Other |
| Start date | Date the plan begins. |
| End date | Date the plan ends. This field is automatically set based on the choice made in the **Timeframe** field. If the **Timeframe** field has **Other**, then enter an end date manually. |
| Assignment | |
| Owning group | Group responsible for owning the plan. |
| Owner | Plan owner. |
| Approvers | People who must approve the plan. |
| Expenses | |
| Budgeted expenses | Budget allocated for the engagements under the plan. |
| Planned expenses | Rolled up planned expenses from the engagements. |
| Actual expenses | Rolled up actual expenses from the engagements. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Expense notes | Notes about the expense details. |
| Resources | |
| Budgeted resources | Number of hours allocated for the engagements under the plan. |
| Planned resources | Rolled up planned resources from the engagements. |
| Actual resources | Rolled up actual resources from the engagements. |
| Resource notes | Notes about the resource details. |
| Activity | |
| Work notes | Notes for this plan. These notes are for internal use and aren't visible to the customers. |
| Additional comments (Customer visible) | Additional comments about the plan that are visible to the customer. |

5. Save the form.
   You can monitor the state of the plan in the stepper of the Overview page as it progresses through the plan process flow.
6. In the Engagements related list, do one of the following.
   - To add engagements, select **New**.
   - To add existing engagements, select **Add**.
7. Select **Request approval**.
   The state changes from **Draft** to **Awaiting approval**.

### Result
The plan is sent for approval to the approver. After the plan is approved, the form displays the **Approved by** and **Approved on** fields with the values automatically set.

## Create an audit engagement in Audit Workspace

Create an engagement in the workspace and assign it to an audit supervisor. Use the workspace to schedule the engagement, plan the details, and budget the expenses.

### Before you begin
Role required: sn_audit.manager, sn_audit_ws.supervisor

### About this task
As an audit supervisor you can create an engagement to manage the audit information and collect entities, controls, and control tests that are relevant to the audit. You can supervise the audit engagement, monitor its execution, and ensure its completion on time as directed.

### Procedure
1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Click the **Create** list and select **Engagement** from the **Home** page.
   You can also create an engagement by navigating to the Audit workspace List page.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Click the lists icon (  ).

b. Click **All engagements** or **My engagements** in the Execution list.

c. Click **New**.

3. On the form, fill in the fields.

**Create New Engagement form**

| Field | Description |
|---|---|
| Number | Unique identification number of the engagement. |
| Name | Name of the engagement. |
| Type | Audit type based on its specific use in the engagement. |
| State | State of the engagement. The default state is Scope. |
| Fieldwork complete (%) | Percentage of the engagement that is complete. |
| Description | General description of the engagement. |
| Objectives | Stated objectives of the engagement. |
| Assignment | |
| Engagement lead | Audit supervisor who oversees and completes the engagement as per directions. |
| Auditors | Auditors assigned to the engagement. |
| Approvers | Approvers assigned to the engagement. |
| Engagement schedule | |
| Fieldwork planned start | Estimated start date of the engagement. |
| Fieldwork planned end | Estimated end date of the engagement. |
| Fieldwork planned duration | Number of days and hours planned for fieldwork. The duration and planned start date of fieldwork are used to calculate the planned end date. If audit tasks are defined, this field is automatically set to the longest planned duration from the audit tasks. |
| Fieldwork actual start | Actual start date of the fieldwork. If audit tasks are defined, this field is automatically set to the earliest actual start date from the audit tasks. |
| Fieldwork actual end | Actual end date of the fieldwork. If audit tasks are defined, this field is automatically set to the latest actual end date from the audit tasks. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Fieldwork actual duration | Duration of fieldwork start date and end date. |
| Plan details | |
| Parent plan | Plan that is to be associated with the engagement. |
| Start date | Start date of the plan. |
| End date | End date of the plan. |
| Expenses and resources | |
| Budgeted expenses | Calculated expenses for the engagement. |
| Planned expenses | Estimated expenses for the engagement. |
| Actual expenses | Actual expenses incurred. |
| Budgeted resources | Budgeted resources for the engagement, in days,hours, minutes, and seconds. |
| Planned resources | Estimated resources for the engagement, in days,hours, minutes, and seconds. If resource plans are defined, this field is automatically set. |
| Actual resources | Actual resources for the engagement, in days,hours, minutes, and seconds. |
| Results | |
| Result | Results of the engagement. The choices are as follows:<br>◦ Satisfactory<br>◦ Adequate<br>◦ Inadequate |
| Opinion | Justification for the selected result. |
| Report | |
| Report template | Template used to generate the knowledge base article that reports the engagement results. |
| Report knowledge base | Knowledge base to be used. |
| Report | Report that contains the engagement results. |
| Activity | |
| Additional comments | Comments that customers can also view. |
| Work notes (Private) | Comments that only the administrator and audit supervisor can view. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | or confidential groups of users can access the record.<br><br>For more information on the confidential option, see Confidentiality flag for audit and compliance records. |

4. Click **Save**.
   You can define the entities that are involved in the audit engagement.
5. From the **Overview** page, click the **Other issues** tab.
   You can add existing one or more related issues to the engagement that you created. By mapping the existing issues to the engagement, you can reduce the count of open issues.

   a. Click the **Add** button.

   b. Select a related issue or issues from the Issues pop-up.

   c. Click **Add**.
   The selected issues are added to the engagement as related issues and an m2m relationship is created between the engagement and the issues in the Issue to Engagement [sn_grc_m2m_issue_engagement] table. You can also create an issue for the engagement by clicking the **New** button, which takes you to the Create New Issue form.

   d. To remove an issue that is mapped to the engagement, select the issue and click **Remove**.
   The remove action only removes the mapping or the association between the engagement and the issue in the m2m table and does not delete the issue record.

   **Note:** The UI action buttons such as New, Add, Remove are not available if the engagement is in the Retired state.

### Manage an engagement from the overview page

After you create and save an engagement with the basic information such as the description, dates, scope, and the objectives, you can see the overview page.

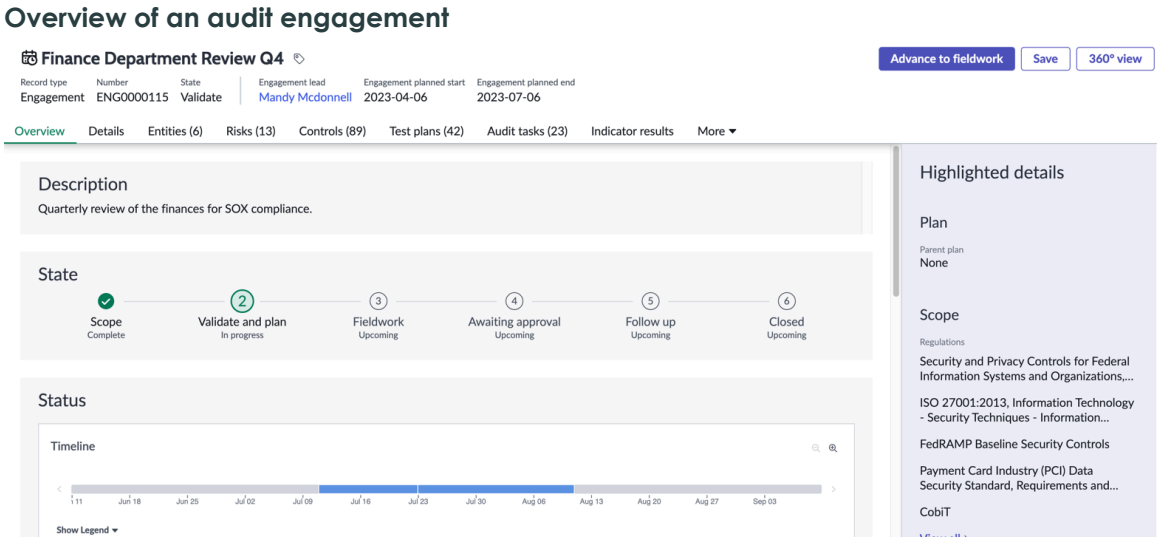
## Overview page of an audit engagement

Use the overview page to get the necessary details and monitor the state flow of the audit engagement in the stepper. You can

- define and scope an audit engagement
- assign team members to it
- perform and review fieldwork
- manage issues
- complete the audit engagement using the different related items

Select the  icon to view the scope of the engagement.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## Create an auditable unit and scope entities at risk

Create auditable units to identify business entities that can possibly be at risk and scope them into audits.

### Before you begin

Role required: sn_audit.manager, sn_audit_ws.supervisor, sn_audit.user, sn_audit_ws.auditor

### About this task

Auditable units are a combination of different entities such as business units, products or services, legal entities, regulatory required audits, processes, programs, systems, policies, regulation, financial statements, and others.

After you determine the nature and scope of the auditable units, your goal is to perform risk assessments, and scope auditable units and entities based on the risk rating.

See also Perform advanced risk assessment in the Risk workspace.

### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Click **Create** and select **Auditable unit** from the **Home** page.
   You can also create an auditable unit by navigating to the Audit workspace List page.
   a. Click the lists icon ( ).
   b. Click **All auditable units** or **My auditable units** in the Scoping list.
   c. Click **New**.
3. On the form, fill in the fields.

#### Create New Auditable Unit form

| Field | Description |
|---|---|
| Number | Unique number of the auditable unit. |
| Name | Name of the auditable unit. For example, Accounts Payable – Finance. |
| State | State of auditable unit. The default state is **Draft**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Priority | Priority of the auditable unit. |
| Description | Brief description of the auditable unit. |
| Assignment | |
| Owning group | Group that owns the auditable unit. |
| Owner | Owner of the auditable unit. |
| Risk assessment | |
| Method | Type of risk assessment to obtain the risk rating of the auditable unit. The choices are:<br>◦ Basic Risk Assessment: Allows you to manually enter a value for the risk rating.<br>◦ Detailed Risk Assessment: Appears when the Advanced Audit plugin is activated. When you select this option, the Risk Assessments related list appears. |
| Risk rating | Risk rating of the auditable unit obtained from a basic risk assessment. |
| Inherent risk rating | Inherent risk score. The value in this field is derived from advanced risk assessment. This field appears if the risk assessment method is **Detailed Risk Assessment**. |
| Control effectiveness | Control effectiveness score. The value in this field is derived from advanced risk assessment. This field appears if the **Method** field has **Detailed Risk Assessment**. |
| Residual risk rating | Residual risk score. The value in this field is derived from advanced risk assessment. This field appears if the **Method** field has **Detailed Risk Assessment**. |

4. Click **Save**.
5. To add entities such as business units, department, vendors, products, business processes, and others to the auditable unit, click the respective related list in the Details page.
6. Select the records from the respective pop-up.
7. Click **Add**.
8. Click **Activate**.
   The state of the auditable unit becomes Active.
9. To retire the auditable unit, click the **Retire** button in the more actions icon ( ••• )
10. If you have GRC: Advanced Risk application installed and if you have selected Risk Assessment Method as **Detailed Risk Assessment**, then you can assess risk by clicking the **Assess risk** button.
    For more information, see risk assessment method in Create an auditable unit.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create a milestone for an engagement

Create a milestone for an engagement to track the progress of an engagement. You can also add audit tasks to a milestone.

## Before you begin

Role required: sn_audit.manager, sn_audit_ws.supervisor

## About this task

A milestone is used to track the progress of an engagement.

After you create milestones for an engagement, you can also add audit tasks to the milestone. You can track those tasks as milestones.

You can assign a milestone to a user who is responsible for the milestone. The assigned user must have the sn_audit.user role. The assigned user then receives a notification about the assignment.

If an engagement moves to the Follow Up state, and if there are no open audit tasks, open milestones, or open observations, then the engagement moves to the **Closed** state.

## Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the lists icon ( ).
3. Select **All engagements** or **My engagements** in the Execution list.
4. Select the link to the engagement record in the **Name** column.
5. Select the **Milestones** tab.
6. Select **New**.
7. On the form, fill in the fields.

### Create New Milestone form

| Field | Description |
|---|---|
| Number | Unique number of the milestone. This number is automatically generated. |
| Name | Name of the milestone. |
| Parent | Parent engagement of the milestone. |
| Type | Audit milestone type. The choices are:<br>◦ Scoping<br>◦ Planning<br>◦ Fieldwork<br>◦ Follow up<br>◦ Reporting<br>◦ Closure |
| State | State of the milestone. The default state is **Open**. |
| Percent complete | Percentage of milestone completed. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | When a value is entered in this field, the state changes to **Work in progress**. |
| Key milestone | Option to mark the milestone as important. |
| Auto complete and close | Option to mark the milestone as close complete when all the associated audit tasks are completed and closed.<br><br>If this option is enabled, then the percent complete is automatically updated according to the number of tasks marked as closed complete. |
| Description | Brief description of the milestone. |
| Assignment | |
| Assignment group | Group responsible for the milestone.<br><br>The group members must have the sn_audit.user role assigned. |
| Assigned to | Person responsible for working on the milestone. |
| Schedule | |
| Due date | Expected completion date of the milestone. |
| Completion date | Actual completion date of the milestone. |
| Closed date | Actual close date of the milestone. |
| Activity | |
| Additional comments | Comments that customers can also view. |
| Work notes (Private) | Comments that only the administrator and audit supervisor can view. |

8. Select **Save**.
   You can view the description of the Milestone record and monitor its status in the **State** banner of the default Overview page.

### Audit task management in Audit Workspace

Audit tasks are completed throughout an engagement and provide documented evidence that the organization is complying with external regulations and internal policies.

Audit tasks can be:

- Control test
- Activity
- Interview
- Walkthrough

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

These audit tasks are assigned to the engagements that are in **Validate** or **Fieldwork** state.

When audit tasks are created or reassigned, a notification is sent to the assigned user. A notification is also sent when the task reaches 75% of its planned duration.

### Create a control test from an engagement

Create a control test that runs periodically and provides documented evidence of whether the associated control is operating correctly or not.

#### Before you begin

Role required: sn_audit.manager, sn_audit_ws.supervisor

#### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the lists icon (  ).
3. Select **All engagements** or **My engagements** in the Execution list.
   Assign an audit task to an engagement that is in one of the following states:
   - Validate
   - Fieldwork
4. Select the link to the engagement record in the **Name** column.
   The engagement record details open in the **Overview** tab.
5. Select the Audit tasks related list.
6. Click the grouped button below the related lists and select **New control test** from the list.
7. On the form, fill in the fields.

**Create New Control test form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the control test. |
| Parent | Parent engagement. |
| Test plan | Test plan associated with this control test. |
| State | State of the control test. The default state is **Open**. |
| Control effectiveness | Control effectiveness. |
| Issue | Issue related to this control test. |
| Assignment | |
| Assigned to | User assigned to the control test. |
| Schedule | |
| Planned start date | Intended start date of the control test. |
| Planned end date | Intended end date of the control test. |
| Planned duration | Expected duration of the control test. As with actual duration, the planned duration |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | shows total activity time and takes the control test schedule into consideration. |
| Actual start date | Actual start date of the control test. |
| Actual end date | Actual end date of the control test. |
| Actual duration | Duration of the control test from control test start to control test closure. |
| Design test | |
| Design effectiveness | ◦ None<br>◦ Effective<br>◦ Ineffective |
| Design expectations | Basic requirement that should be met for a control to be effective. This field checks if the control was designed properly to achieve the control objective. |
| Design assessment procedures | Procedure or steps to be followed to conclude whether the design of the control is effective to achieve the control objective or not. This procedure is based on the design expectation. |
| Design results | Results of testing the design of the control based on the design assessment procedure. |
| Operational test | |
| Operating effectiveness | ◦ None<br>◦ Effective<br>◦ Ineffective |
| Operational expectations | Expectations that should be met to ensure that the control is operating effectively to achieve the control objective. |
| Operational assessment procedures | Detailed steps, to carry out the operational expectations, which must be performed to conclude that the control is operating successfully. |
| Operational results | Results of testing the operation of the control based on the operation assessment procedure. |
| Activity | |
| Work notes (Private) | Comments that the audit manager and audit supervisor can only view. |
| Additional comments | Comments that customers can also view. |
| Confidentiality | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on the confidential option, see Confidentiality flag for audit and compliance records. |

8. Select **Save**.
   You can view the description and monitor the state of the control test in the **State** banner of the Overview page as the record progresses through the control test process flows.

### Create an activity in the Audit Workspace

Create an activity that explores and provides documented evidence of whether the associated control is operating correctly or not.

### Before you begin

Role required: sn_audit.manager, sn_audit_ws.supervisor

### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the lists icon ( ).
3. Select **All engagements** or **My engagements** in the Execution list.
   Assign an audit task to an engagement that is in one of the following states:
   - Validate
   - Fieldwork
4. Select the link to the engagement record in the **Name** column.
   The engagement record details open in the **Overview** tab.
5. Select the Audit tasks related list.
6. Click the grouped button below the related lists and select **New activity** from the list.
7. On the form, fill in the fields.

#### Create New Activity form

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the activity. |
| Parent | Parent audit task or parent engagement. |
| State | State of the activity. The default state is **Open**. |
| Description | Detailed description of the activity. |
| Assignment | |
| Assigned to | User assigned to the activity. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Schedule | |
| Planned start date | Intended start date of the activity. |
| Planned end date | Intended end date of the activity. |
| Planned duration | Expected duration of the activity. As with actual duration, the planned duration shows total activity time and takes the activity schedule into consideration. |
| Actual start date | Actual start date of the activity. |
| Actual end date | Actual end date of the activity. |
| Actual duration | Actual duration of the activity from its start to its closure. |
| Activity | |
| Additional comments | Comments that customers can also view. |
| Work notes (Private) | Comments that the audit manager and audit supervisor can only view. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on the confidential option, see Confidentiality flag for audit and compliance records. |

8. Select **Save**.
   You can monitor the status of the activity in the **State** banner of the Overview page.

### Create an interview in Audit Workspace

Create an interview with control owners to discuss and provide documented evidence of whether the associated control is operating correctly or not.

#### Before you begin

Role required: sn_audit.manager, sn_audit_ws.supervisor

#### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the lists icon ( ).
3. Select **All engagements** or **My engagements** in the Execution list.
   Assign an audit task to an engagement that is in one of the following states:
   - Validate
   - Fieldwork
4. Select the link to the engagement record in the **Name** column.
   The engagement record details open in the **Overview** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Select the Audit tasks related list.
6. Click the grouped button below the related lists and select **New interview** from the list.
7. On the form, fill in the fields.

**Create New Interview form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the interview. |
| Parent | Parent engagement. |
| State | State of the interview. The default state is **Open**. |
| Description | Detailed description of the interview. |
| Assignment | |
| Assigned to | User assigned to the interview. |
| Primary contact | User to be contacted for the interview. |
| Other contacts | Other users to be contacted, if the primary contact is unavailable. |
| Notes | Additional notes about the interview contacts. |
| Schedule | |
| Planned start date | Intended start date of the interview. |
| Planned end date | Intended end date of the interview. |
| Planned duration | Expected duration of the interview. As with actual duration, the planned duration shows total activity time and takes the interview schedule into consideration. |
| Actual start date | Actual start date of the interview. |
| Actual end date | Actual end date of the interview. |
| Actual duration | Actual duration of the interview from its start to its closure. |
| Activity | |
| Additional comments | Comments that customers can also view. |
| Work notes (Private) | Comments that the audit manager and audit supervisor can only view. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | For more information on the confidential option, see Confidentiality flag for audit and compliance records. |

8. Select **Save**.
   You can monitor the state of the interview audit task in the **State** banner of the Overview page as the record progresses through the different process flows.

### Create a walkthrough in the Audit Workspace

Create and conduct a walk through to observe and provide documented evidence of whether the associated control is operating correctly or not.

**Before you begin**
Role required: sn_audit.manager, sn_audit_ws.supervisor

**Procedure**

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the lists icon ( ).
3. Select **All engagements** or **My engagements** in the Execution list.
   Assign an audit task to an engagement that is in one of the following states:
   - Validate
   - Fieldwork
4. Select the link to the engagement record in the **Name** column.
   The engagement record details open in the **Overview** tab.
5. Select the Audit tasks related list.
6. Click the grouped button below the related lists and select **New walkthrough** from the list.
7. On the form, fill in the fields.

#### Create New Walkthrough form

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the walkthrough. |
| Parent | Parent engagement. |
| State | State of the interview. The default state is **Open**. |
| Description | Detailed description of the walkthrough. |
| Assignment | |
| Assigned to | User assigned to the walkthrough. |
| Primary contact | User to be contacted for the walkthrough. |
| Other contacts | Other users to be contacted, if the primary contact is unavailable. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Schedule | |
| Planned start date | Intended start date of the walkthrough. |
| Planned end date | Intended end date of the walkthrough. |
| Planned duration | Expected duration of the walkthrough. As with actual duration, the planned duration shows total activity time and takes the walkthrough schedule into consideration. |
| Actual start date | Date on which the walkthrough began. |
| Actual end date | Date on which the walkthrough ended. |
| Actual duration | Duration of the walkthrough from its start to end. |
| Walkthrough | |
| Execution steps | Details of activities to be performed during the walkthrough. |
| Explanation | Intended purpose of the walkthrough. |
| Additional information | Additional information the user conducting the walkthrough must be aware of. |
| Results | Details of what transpired during the walkthrough. |
| Activity | |
| Additional comments | Comments that customers can also view. |
| Work notes (Private) | Comments that the audit manager and audit supervisor can only view. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on the confidential option, see Confidentiality flag for audit and compliance records. |

8. Select **Save**.
   You can view the description of the walkthrough and monitor its status in the **State** banner of the Overview page.

### Add entities to an engagement scope and validate the engagement

Add entities related to the selected auditable units to the engagement. In addition, you can also add entities other than the ones created for auditable units to the engagement.

**Before you begin**
Role required: sn_audit.manager, sn_audit_ws.supervisor

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

During the **Scope** state, as an audit supervisor you can define which entities are involved in the audit engagement. For example, for a financial audit, you can include all business services that the finance department relies on and the finance department itself.

When you add an entity to an engagement, the corresponding risks, controls, test plans, and indicator results of the entity are also added to the engagement.

### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Click the lists icon ( ).
3. Click **All engagements** or **My engagements** in the Execution list.
   You can scope entities to an engagement that is in **Scope** state.
4. Click the link to the engagement record in the **Name** column.
   The engagement record details open in the **Overview** tab.
5. Click the Entities related list.
6. Click the **Add auditable units** button.
7. In the Auditable units pop-up, select the desired entities that are included in the audit engagement.
   These auditable units are those that have entities already created.
8. Click **Add**.
   If there are risks and controls, test plans, and indicator results associated with an entity then they appear in their respective sections.

   Risks, controls, and test plans are automatically added if the engagement is already in the **Validate** state. Other related items are added only when you click **Validate** or **Validate and plan** button.

   **Note:** If you do not have GRC: Advanced Audit application installed, only then the **Validate** button appears, otherwise the **Validate and plan** button appears.

   After adding the auditable units as entities to the audit engagement, you can validate and plan the engagement.
9. To add entities other than the ones created for auditable units, click the **Add other entities** button.

   **Note:** If you have GRC: Advanced Audit application installed, only then the **Add auditable units** and **Add other entities** fields appear. Otherwise, an **Add** button appears in the page.
10. Click the **Validate and plan** button.
    After an engagement has moved to the **Validate** state, all the risks, controls, and test plans associated with the entities in the engagement's scope are associated with the audit. Indicator results that were collected during the audit period of the engagement are also associated with the audit. As an audit supervisor, you can review the risks, controls, test plans, and indicator results, and update the scope of the engagement, if necessary. You can also begin creating and planning audit tasks for the engagement.

## Create an issue for an engagement

Create an issue to document policy, risk, or audit observations, or to accept any GRC problems. You can also identify the source of the issue to help analyze and classify the issues.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_audit.manager, sn_audit_ws.supervisor

### Procedure
1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Click the lists icon (  ).
3. Click **All engagements** or **My engagements** in the Execution list.
4. Click the link to the engagement record in the **Name** column.
   The engagement record details open in the **Overview** tab.
5. Click the Other issues related list.
6. Click **New**.
7. On the form, fill in the fields.

**Create New Issue form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the issue. |
| Issue source | Source from where the issue was created. This field is auto-populated with one of the following options based on how the issue is created:<br>◦ Indicator Failure: Issue is created by a failure of the indicator.<br>◦ Risk Assessment: Issue is created in a risk.<br>◦ Risk Event: Issue is created in a risk event.<br>◦ Control Attestation Failure: Issue is created due to a non-compliant control.<br>◦ Control Test Failure: Issue is created when a control is ineffective and the control test is marked as closed and complete.<br>◦ Ad-hoc: Issue is manually created. |
| Issue type | Type of issue. |
| Classification | Classification of the issue as a risk, compliance, or audit, based on the issue type. |
| State | ◦ New<br>◦ Analyze<br>◦ Respond<br>◦ Review<br>◦ Closed Complete<br>◦ Closed Incomplete |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Substate | Substate and applicable details for the substate. |
| Priority | Sequence in which an issue needs to be resolved, based on its impact and urgency:<br>◦ 1 — Critical<br>◦ 2 — High<br>◦ 3 — Moderate<br>◦ 4 — Low<br>◦ 5 — Planning |
| Issue rating | Issue manager can assign a issue rating to the issue. Based on the issue rating, the **Due date** in the **Dates** tab is calculated as follows and displayed:<br>◦ Very high (2 days)<br>◦ High (4 days)<br>◦ Moderate (8 days)<br>◦ Low (10 days)<br>◦ Very Low (15 days)<br>You can manually override the **Due date**. |
| Description | Comprehensive description of the issue. |
| Assignment | |
| Assignment group | Group to which the issue is assigned. Each member receives a notification when an activity occurs on this issue. |
| Assigned to | Member of the group assigned to resolve the issue. |
| Issue manager group | Group responsible for managing and reviewing the issue. |
| Issue manager | User responsible for managing and reviewing the issue. |
| Watch list | Users added to view the issue. |
| Schedule | |
| Due date | Due date is auto-populated based on a GRC property, *`Auto populate due date based on issue rating`*. If it is set to **Yes**, the field is auto-populated based on the predefined remediation time frame for the issue's risk rating. Otherwise, you can manually enter a due date.<br>When an issue transitions to the **Respond** state, an entry in this field is mandatory. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Confirmed date | Date on which the issue is confirmed. This field is read-only, and displays the current date when the issue is moved from **New** to any of the following states:<br>◦ Analyze<br>◦ Review<br>◦ Respond<br>**Note:** If a triage issue is converted to an actual issue, this field displays the date it was converted. |
| Created | Date and time the issue was created. |
| Closed | Date and time the issue was closed. |
| Planned start date | Date and time when the work on the issue is expected to begin. |
| Planned end date | Date and time when the work on the issue is expected to end. |
| Planned duration | Estimated duration of work time. Calculated using the **Planned start date** and **Planned end date**. |
| Actual start date | Time when work began on the issue. |
| Actual end date | Time when work on the issue was completed. |
| Actual duration | Duration of work time. Calculated using the **Actual start date** and **Actual end date**. |
| Details | |
| Control/Risk | Control or risk associated with the issue. |
| Control Objective/Risk statement | Control objective or risk statement related to this issue. |
| Entity | Related entity. |
| Configuration item | Item associated with the issue. If all child issues have the same configuration item, it gets copied over to the parent issue. |
| Location | Location where the issue occurred. |
| Risk event | Related risk event. |
| Engagement | Related engagement. |
| Policy | Policy associated with the issue. |
| Authority document | Authority document associated with the issue. |
| Issue grouping | |
| Parent issue | Parent issue to which the issue belongs. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Issue group rule | Group rule assigned to the issue.<br><br>Issue group rule is used to group similar issues together into a parent issue based on conditions defined in the rule. This allows you to work on similar issues simultaneously and close out the parent issue after all issues are resolved. This closes out all the child issues. |
| Action plan | |
| Recommendation | Resolution actions recommended by the risk, compliance, or audit teams. |
| Action plan | Plan for remediating the issue. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |
| Activity | |
| Work notes (Private) | Information about how to resolve the issue, or steps already taken to resolve it, if applicable. Work notes are visible to users who are assigned to the issue. |
| Additional comments | Public information about the issue. |

8. Click **Save**.

### Request evidence during audits using Audit Workspace

Request evidence at any stage during an audit using the Audit Workspace. The details about the items for which evidence is requested are also provided to the person responsible for providing the evidence.

#### Before you begin

Role required: sn_audit.user

#### Procedure

1. Navigate to **All** > **Audit Workspace**.
2. In the Audit Workspace select the List icon ( ).
3. Navigate to **Evidence requests** > **My request**.
4. Select **New**.
5. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Evidence request form

| Field | Description |
|---|---|
| Number | Unique number of the evidence request. |
| Name | A name for this request. |
| Requester | User requesting evidence. This field is automatically populated. |
| Requested on behalf of | User for whom evidence is being requested. |
| Type | Type of evidence that is created. Can be either Audit or Compliance. |
| Request reason | Reason for requesting evidence. |
| State | State of the request. The default state is **Draft**. |
| Substate | An additional state for the request. |
| Description | Detailed description of the evidence request. |
| Assignment | |
| Assignment group | Group assigned to provide evidence. |
| Assigned to | User responsible for providing the evidence. |
| Watch list | Users interested in viewing the evidence collected. If a person is added on the watch list, they can navigate to **Audit** > **Evidence Request** > **Watched Evidence Requests** to view the requests. |
| Schedule | |
| Due date | Expected date of evidence submission. |
| Opened | Date the request is opened. This date is automatically updated. |
| Closed | Date the request is closed. This date is automatically updated. |
| Activity | |
| Work notes | Type any notes that might be required. |
| Activities | Activity log for the request. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on the confidential option, see Confidentiality flag for audit and compliance records. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Save the form.
   Monitor the state of the Evidence in the stepper of the Overview page. The record progresses through a sequence of logical steps when you accept evidence, request revision of the evidence, and request information.

   The Evidence collection details related list appears. This related list is used to list the items for which evidence is requested.

7. Select **New**.
8. On the form, fill in the fields.

**Evidence collection details form**

| Field | Description |
|---|---|
| Number | Unique number for the evidence collection detail. |
| Name | A name for this request. |
| Evidence collection type | Record for which evidence is requested.<br><br>If you're a user with the audit user role, the available options are:<br>◦ Audit task<br>◦ Authority document<br>◦ Citation<br>◦ Control<br>◦ Control objective<br>◦ Control test<br>◦ Engagement<br>◦ Entity<br>◦ Issue<br>◦ Policy<br><br>If the request was entered by a user with the audit user role, the available options are:<br>◦ Audit task<br>◦ Control<br>◦ Control objective<br>◦ Control test<br>◦ Engagement<br>◦ Entity<br>◦ Issues |
| Evidence for | Lists all the tables to which the evidence is applied. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Evidence request | Unique number of the evidence request task. |
| Assignment | |
| Assignment group | Group assigned to provide evidence. The users of this group must have the sn_grc.business_user roles. |
| Assigned to | User responsible for providing evidence. |
| Instructions | |
| Evidence collection instructions | Instructions for providing evidence. For example, list of supporting documents, files, and so on. |

9. Select **Save**.
10. Select **Request Evidence**.
    When an evidence request is already in the Work in Progress state, and a new evidence collection detail is added, the evidence request task is sent to the assignee immediately. The Evidence related list appears with the list of evidences and the person who is assigned the request receives an email notification to provide the requested evidence. Also, the state of the request changes to **Work in Progress**.You can view the description. Monitor the state of the Evidence request in the stepper of the Overview page as it progresses through the evidence request process flow.

### Audit observations in Audit Workspace

Audit observations are the results of an audit. As an important part of the audit report, audit observations represent the results of reviews, analysis, interviews, and discussions.

## Overview of an audit observation

Audit observations are used to bring significant issues to the attention of audit supervisors. Observations are logged in the system. For example, if a bank's operations are being audited, then the audit observations are based on evidence about how the bank's operations perform against the audit criteria. During control testing, interviews, and walkthroughs, audit observations are recorded. An audit user can create an observation from an engagement if the engagement is not in the **Follow Up** or **Closed** states. An observation can also be created from all types of audit tasks.

After the auditor completes the audit, the auditor then presents the audit observations to the audit supervisors. By using the audit observations, the auditor can present a summary of problems, discoveries, and recommendations. The audit team reviews the observations to determine if the observation is a reportable issue. The audit team can also determine if the observation can be tracked as a recommendation, an observation, or a best practice.

In its life cycle, an audit observation moves through the following states:

1. Draft
2. Review
3. Respond
4. Finalize
5. Closed

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Status workflow of an audit observation in workspace

1. An audit user with the role sn_audit.user creates an observation. See Create an observation for an engagement.
   a. To create an observation, navigate to **All** > **Audit** > **Audit Workspace**.
   b. Click the lists icon (  ).
   c. Click **All engagements** or **My engagements** in the Execution list.
   d. Click the link to the engagement record in the **Name** column.
   e. Click the **Observations** tab.
   f. Click **New**.
   g. On the Create New Observation form, fill in the fields.
2. The observation creator assigns respondents and peer reviewers to the observation. The respondents are the entity owners and control owners. The peer reviewers are the auditors and audit leads of the engagement.
3. The observation creator can request a peer review of the observation. In that case, the following happens:
   a. The peer reviewer gets a notification to perform the peer review. The peer reviewer can view the task under **My pending tasks** > **All** by clicking the tasks icon (  ) in the workspace.

      **Note:** The peer reviewer can also navigate to **Tasks** > **My tasks** > **Open** in the Home page of the workspace.

   b. The peer reviewer completes the review.

      **Note:** When a peer review is requested, the state remains as **Draft** but the substate changes to **Peer review requested**.

4. The observation creator can also request a review. The reviewer can be an audit supervisor or the audit lead.
   a. The reviewer gets a notification to perform the review. The reviewer can view the task by navigating to **My pending tasks** > **All** > **Observations**.
   b. The reviewer can either request a revision of the observation or request a response from the respondent. The reviewer can also provide feedback in the **Results** section by selecting the appropriate option.
5. If the reviewer requested a response from the respondent, then the respondent responds to the observation by navigating to **Audit** > **Observations** > **My Pending Response**.
6. The observation moves to the **Finalize** state.
7. The observation is closed and an issue is created.

### Create an observation for an engagement

Create an audit observation to present a summary of problems, discoveries, and recommendations. The audit team can then review the observations to determine if the observation is a reportable issue.

**Before you begin**
Role required: sn_audit.manager, sn_audit_ws.supervisor, sn_audit.user, sn_audit_ws.auditor

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the lists icon ( ).
3. Select **All engagements** in the Execution list.
4. Select the link to the engagement record in the **Name** column.
5. Select the **Observations** tab.
6. Select **New**.
7. On the form, fill in the fields.

**Create New Observation form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the observation. |
| Engagement | Engagement associated with this observation. |
| Source | Source or origin of the observation. |
| Issue type | Reason for creating the observation. The choices are:<br>◦ Control design effectiveness failure<br>◦ Control operative effectiveness failure<br>◦ Control does not exist<br>◦ Control doesn't meet requirement<br>◦ Other observation |
| State | State of the observation. |
| Substate | Substate of the observation. |
| Priority | Priority of the observation. Choices are:<br>◦ 1 — Critical<br>◦ 2 — High<br>◦ 3 — Moderate<br>◦ 4 — Low |
| Description | Detailed description of the observation. |
| Action plan | Plan for resolving the resulting issue. |
| Assignment | |
| Owner | User who creates and is responsible for the observation. |
| Peer reviewer | One of the auditors responsible for peer review. |
| Respondent | User responsible for completion of the action plan. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | Respondent can be the owner of the entity or control associated with the parent engagement. |
| Reviewer group | Group assigned to review the observation. |
| Reviewer | User responsible for reviewing the observation. |
| Watch list | Users interested in following updates to the observation. |
| Details | |
| Control | Control associated with the observation. |
| Control Objective | Control objective associated with the observation. |
| Entity | Entity associated with the observation. |
| Audit task | Audit task associated with the observation. |
| Results | |
| Result | Result of the observation. The choices are as follows:<br>◦ Track as an observation<br>◦ Track as a recommendation<br>◦ Track as a best practice<br>◦ Confirmed as a new issue<br>◦ Confirmed as an existing issue<br>◦ No action required |
| Explanation | Explanation for the selected result. |
| Activity | |
| Work notes (Private) | Notes about the observation. Work notes are visible to users who are assigned to the observation. |
| Additional comments | Public information about the observation. |
| Security | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record. |

Confidentiality flag to control access of audit records

You can set the confidentiality flag at the record level for an issue, engagement, observation, control test, activity, interview, and walkthrough records. The users whom you determine to view and update these records are confidential users.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the **Confidentiality** option is selected, a list of users who can be an engagement lead, auditors, and approvers are auto-populated as **Confidential users**.

You can add more audit users or GRC business users to the list or remove some of the existing users based on your access control criteria and can set them as confidential users.

Additionally, you can also add random users to the record, who are neither audit users nor GRC business users. However, an email notification is sent to all confidential users who have neither an audit user nor a GRC business user role intimating them to acquire the confidential role (sn_grc.confidential_user) from the admin if they are to access the record.

You can also select groups as **Confidential groups** who can access the record as well. For more information, see Confidential records in GRC common features.

To enable the Confidentiality property at the system level:

**a.** Navigate to **System Properties** > **All Properties**.

**b.** Select *sn_grc.enable_record_confidentiality* system property.

**c.** Enter **true** in the **Value** field. This action enables record level confidentiality.

**d.** Select **Update**.

**8.** Select **Save**.
You can monitor the state of the observation record in the **State** banner of the default Overview page as the record progresses through the different states.

## Approve or reject an engagement in Audit Workspace

If you are an audit user and are assigned as an approver for an engagement, you can approve or reject an engagement in the **Awaiting Approval** state.

### Before you begin

Role required: sn_audit.user, sn_audit_ws.auditor

### Procedure

**1.** Navigate to **All** > **Audit** > **Audit Workspace**.

**2.** Click the tasks icon ( ).
The workspace opens listing all engagements assigned to you including the ones waiting for your approval.

**3.** Click the **Needs my approval** button in the My pending tasks related list.

**4.** Click the link to open the approval record associated with the engagement in the **State** column.

**5.** Click **Approved** or **Rejected** in the **State** list.

**6.** Click **Save**.
One of the following actions occurs:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- If the engagement is approved and there are remaining open tasks or issues, it automatically moves into the **Follow Up** state.
- If the engagement is approved and there are no remaining open tasks or issues, it automatically moves into the **Closed** state.
- If the engagement is rejected, it automatically moves back to the **Fieldwork** state

## Generate a report from an engagement in Audit Workspace

Generate a report that summarizes the findings of an engagement to communicate the report findings to executives.

### Before you begin

Role required: sn_audit.manager, sn_audit_ws.supervisor

### About this task

You can generate a report for engagements that are in the **Awaiting approval**, **Follow up**, or **Closed complete** states.

### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Click the lists icon ( ).
3. Click **All engagements** or **My engagements** in the Execution list.
4. Click the link to the engagement record in the **Name** column.
   The engagement must be in **Awaiting approval**, **Follow up**, or **Closed complete** state.
5. Click the **Details** tab.
6. If you have not entered details in the Report section of the Engagement form, then fill in the fields.

**Report section of the Engagement form**

| Field | Description |
|---|---|
| Report template | Template used to generate the knowledge base article that reports the engagement results. |
| Report knowledge base | Knowledge base to be used. |

7. Click **Save**.
8. To generate the report, click the **Generate report** button.

## Audit Workspace for the Auditor

The auditor workspace is a centralized workspace for managing audit activities.

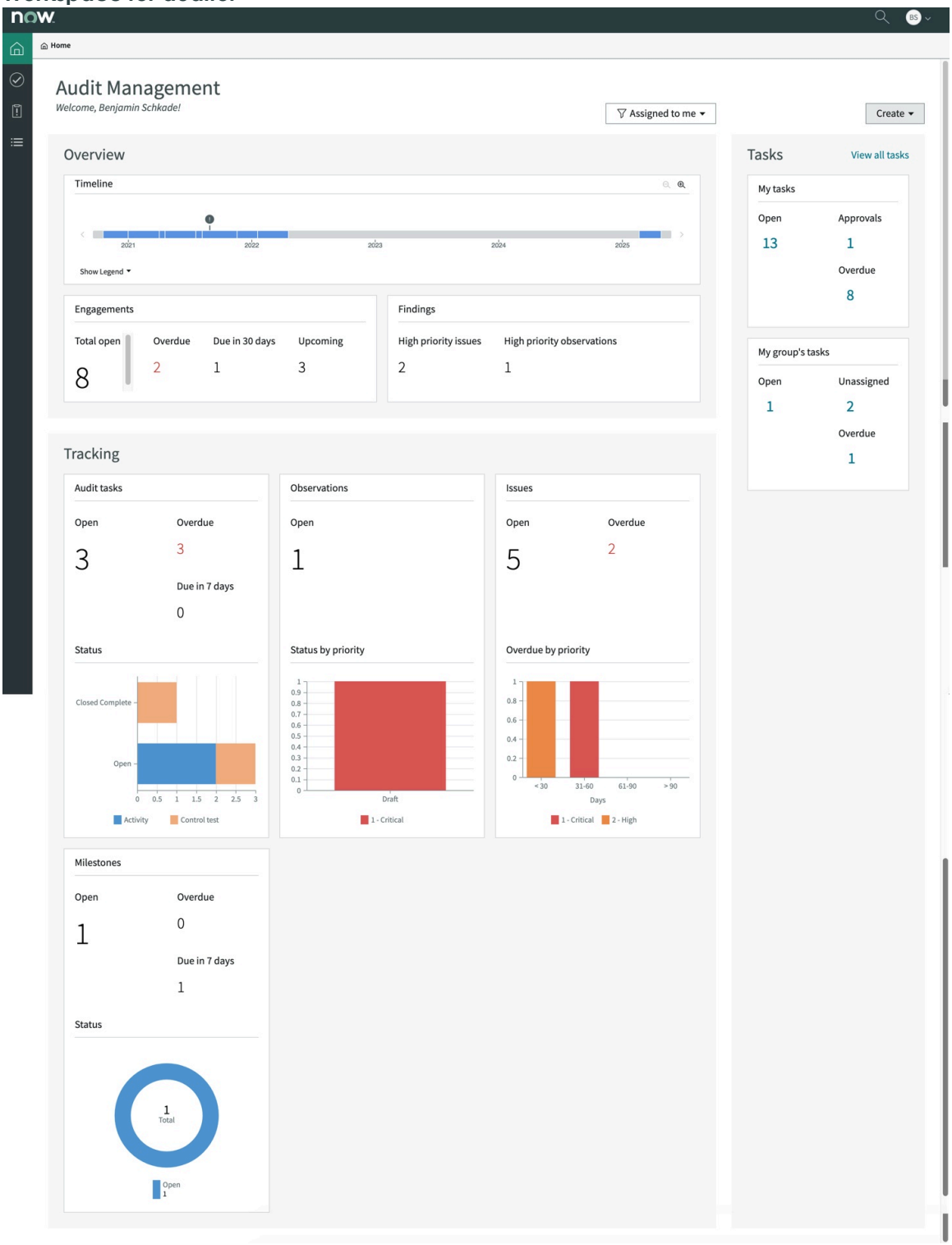
## Overview of auditor workspace

An auditor analyses the operational and financial processes of a company to ensure compliance with industry and federal regulation. They prepare financial reports, review internal controls, collect evidence, conduct audit test, and follow up on audit findings.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Using the auditor workspace, auditors can perform fieldwork such as control tests, activities, interviews, and walkthroughs. They can document their work and findings, and resolve or follow up the audit findings.

### Workspace for auditor




## Tasks of an Auditor

The following table lists the key tasks that you can perform in your role as an auditor.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Tasks of an auditor

| Activity | Task |
|---|---|
| Examine records, reports, operating practices, and documentation to ensure compliance with internal controls. | Update an assigned control test. |
| Create test plans to document control testing procedure. | Create a test plan. |
| Coordinate walkthroughs and interviews for assessing internal control processes. | Update other assigned audit tasks. |
| Request and review evidence for control implementation. | Request evidence for audit tasks. |
| Comply with federal, state, and local security legal requirements. | Create an observation for an audit task assigned to an auditor. |

### Update an assigned control test in Audit Workspace

Use the Audit Workspace to ensure compliance with the established internal control procedures by reviewing records, reports, operating practices, and documentation.

#### Before you begin

Role required: sn_audit_ws.auditor, sn_audit.user

#### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Click the tasks icon ( ).
   The workspace opens listing **All** tasks assigned to you in the My pending tasks related list.
3. Move the state to **Work In progress**, and enter the details.
   You can move the control test to **Review** state if all required information are entered.
4. To approve a control test that requires your approval, click the **Needs my approval** button.

   a. Click the link to open the control test in the **State** column.

   b. Review the control test details and click the **State** list to update the requested control test to an appropriate state.

      The choices are:

      - Not Yet Requested
      - Requested
      - Approved
      - Rejected
      - Cancelled
      - No Longer Required

   c. Click **Save**.

5. Click the **Details** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Review the control test details and click the **State** list to update it to an appropriate state. You can now move the state of the control test to **Close Complete**.
7. Click **Save**.

### Update other assigned audit tasks in Audit Workspace

Update the audit tasks such as walkthroughs and interviews that are assigned to you when you get a notification.

#### Before you begin
Role required: sn_audit_ws.auditor, sn_audit.user

#### About this task
Audit tasks are completed throughout an engagement and provide documented evidence that the organization is complying with external regulations and internal policies.

#### Procedure
1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Click the tasks icon ( ).
   The workspace opens listing **All** tasks in the **My pending tasks** tab. You can view **All – Audit tasks** assigned to you.
3. Click the audit task record either an interview, activity, or a walkthrough that you want to update in the **Name** column.
   The record opens in the **Overview** tab displaying the workflow of its state.
4. Click the **Details** tab to review and update the audit task details.
   In addition to entering other details, you can also move the state of the audit task to **Work In Progress**, **Review**, or **Close Complete**.
5. Click **Save**.

### Create an observation for an audit task

Create an observation for an audit task to comply with federal state and local security legal requirements by studying the existing and new security legislation.

#### Before you begin
Role required: sn_audit_ws.auditor, sn_audit.user

#### About this task
Creating an observation also helps enforce adherence to requirements, thereby advising the management on the needed actions to adhere to the federal and local security legal requirements.

#### Procedure
1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Click the tasks icon ( ).
   The workspace opens listing **All** tasks in the **My pending tasks** tab. You can view **All – Audit tasks** assigned to you.
3. Click the audit task record for which you want to create an observation in the **Name** column.
   The record opens in the **Overview** tab displaying the workflow of its state.
4. Click the **Observations** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **New**.
6. Enter the details in the Create New Observation form.
7. Click **Save**.

## Understanding Audit Management

The Audit Management automates the work streams of internal audit teams, optimizing resources and productivity, and eliminating recurring audit findings. Audit Management uses compliance and risk data to scope, plan, and prioritize audit engagements. The on-going review of policies and procedures, risks, and control breakdowns provide an opportunity for fixing issues before they become audit failures.

### Audit Management users

Auditors (an independent body, typically reporting to the board of directors).

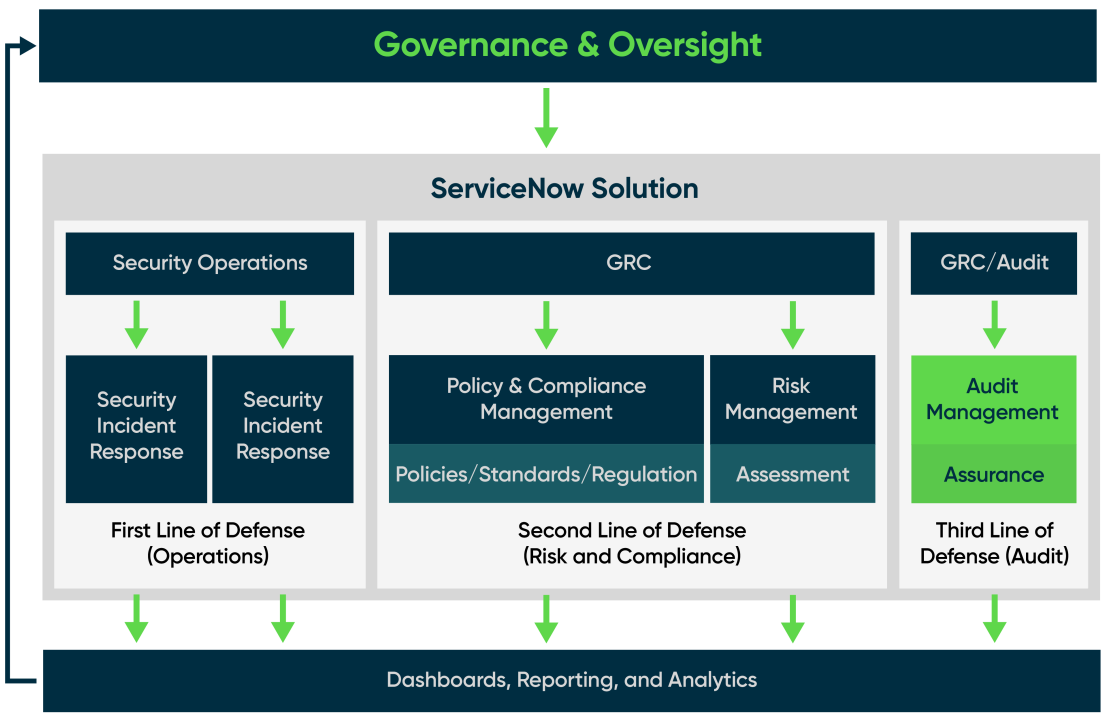
### Key activities for Audit Management

Auditors are responsible for the following:

- Review policies and procedures
- Review risks
- Review control design
- Review control test design
- Review control test results
- Test controls
- Issue observations

### Audit Management and the ServiceNow platform

**Audit Management and the Now Platform**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** For more information on the GRC application nomenclature and industry terminology, see GRC application nomenclature updates and industry terminology.

## Create an audit report template

Create an audit report template to generate an audit report. If you're an audit developer, you can use either the HTML, Script, or XML format to create an audit report template. You can then use the audit report template to display data in an audit report.

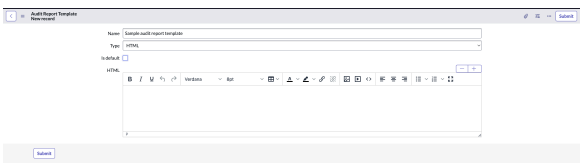
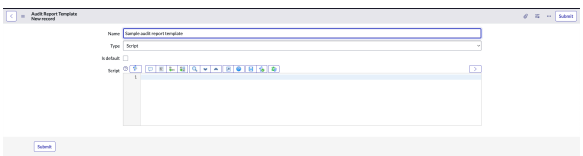
### Before you begin

Role required: sn_audit.developer

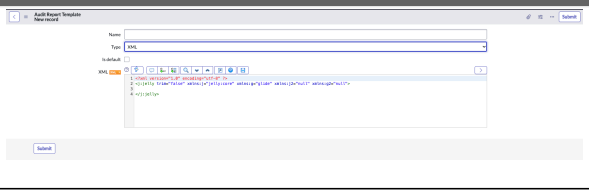
### Procedure

1. Navigate to **All** > **Audit** > **Administration** > **Audit Report Templates**.
2. Click **New**.
3. On the form, fill in the fields.

#### Audit report template form

| Field | Value |
|---|---|
| Name | Name of the audit report template. |
| Type | Type of the audit report template. Available options are:<br>◦ **HTML**<br>◦ **Script**<br>◦ **XML**<br>You can use these formats to generate the audit report template. These templates are used in the audit reports to display data in HTML, Script, or XML format. |
| Is default | Option that indicates that this template is used as the default template for all KB articles. |
| HTML | HTML code. When you select the **HTML** option, you can add the HTML code in the audit report template as shown in the following example:<br>  |
| Script | Script code. When you select the **Script** option, you can add the Script code in the audit report template as shown in the following example:<br>  |
| XML | XML code. When you select the **XML** option, you can add the XML code in your audit report template as shown in the following example: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Value |
| --- | --- |
| |  |

4. Click **Submit**.
   The audit report template is displayed in the list view as shown in the following example:




You can use the audit report template to display data as per the defined format in an audit report.

## Manage test templates and test plans

An audit engagement may include control testing activities during which controls are evaluated for design and operational effectiveness.

## Test Templates and Test Plans

To conduct control testing, before an engagement starts, audit managers create test plans for the relevant controls. Audit managers can use test templates to create multiple test plans for similar controls at one time.

During the **Validate** state of an audit engagement, the test plans that are associated with the controls in the engagement's scope are automatically associated with the engagement. Audit managers can generate control tests from those associated test plans and create individual control tests as needed.

### Create a test template

Test templates allow audit managers to quickly create many test plans using much of the same testing criteria.

#### Before you begin

Role required: sn_audit.admin, sn_audit.manager, or sn_audit.user

#### Procedure

1. Navigate to **All** > **Audit** > **Audit Testing** > **Test Templates**.
2. Click **New**.
3. On the form, fill in the fields.

**Test template form**

| Field | Description |
| --- | --- |
| Number | Unique identification number. |
| Duration | Duration of the test. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Short description | A brief and general description of the test template. |
| Design Test* | |
| Design expectations | Expectations of how a control is designed. |
| Design assessment procedures | Document how to assess if a control is designed effectively. |
| Operation Test* | |
| Operation expectations | Expectations of how a control operates. |
| Operation assessment procedures | Document how to assess if a control is operating effectively |

4. Click **Submit**.

### Relate a test template to a control objective

Audit owners can create generic control test templates for a control objective, avoiding the creation of individual control test plans for every control.

#### Before you begin
Role required: sn_audit.admin or sn_audit.manager

#### Procedure

1. Navigate to **All** > **Audit** > **Audit Testing** > **Test Templates**.
2. Open the test template record.
3. Select a control objective and click **Update**.

### Create an audit test plan

Test plans can be created from scratch or based on test templates and describe how a feature is to be tested.

#### Before you begin
Role required: sn_audit.user, sn_audit.external_auditor

#### Procedure

1. Navigate to **All** > **Audit** > **Audit Testing** > **Test Plans**.
2. Click **New**.
3. On the form, fill in the fields.

#### Test template form

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Control | The control that this test plan covers. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** This field is available only when the Policy and Compliance Management plugin is activated. |
| Test Template | The related test template. |
| Duration | The expected duration of the test. |
| Name | A brief and general description of the test plan. |
| Design Test | |
| Design expectations | Expectations of how a control is designed. |
| Design assessment procedures | Document that shows how to assess if a control is designed effectively. |
| Operation Test | |
| Operation expectations | Expectations of how a control operates. |
| Operation assessment procedures | Document that shows how to assess if a control is operating effectively. |

4. Click **Submit**.

### Create multiple test plans from a test template

If GRC: Policy and Compliance Management is installed, a test template can be used to create test plans for all the controls associated with the control objective of the test plan.

**Before you begin**
Role required: sn_audit.manager or sn_audit.admin

**Procedure**

1. Navigate to **All** > **Audit** > **Audit Testing** > **Test Templates**.
2. Select the test template from which to generate test plans.
3. Click the **Create Test Plans for All Controls** related link.

**Note:** This link is only visible if there are controls associated with the test plan's control objective that have not yet had a test plan generated from the current test template.

## Manage engagements

The audit engagement process involves creating, planning, scoping, and conducting engagements as well as reporting on engagement findings.

## Engagement process

The base system audit engagement process includes steps for scoping, validating, conducting, and approving engagement results. It also contains steps for following up on open audit tasks and issues, and finally closing out the audit engagement.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### States of the engagement process

| State | Description |
|---|---|
| Scope | During the **Scope** state, audit managers define which entities are involved in the audit engagement. For example, for a financial audit, one may include all business services that the finance department relies on and the finance department itself.<br><br>See Add entities to an engagement scope. |
| Validate | After an engagement has moved to the **Validate** state, all the risks, controls, and test plans associated with the entities in the engagement's scope will be associated with the audit. Indicator results that were collected during the audit period of the engagement will also be associated with the audit. Audit managers can review the risks, controls, test plans, and indicator results, and update the scope of the engagement, if necessary. Audit managers can also begin creating and planning audit tasks for the engagement.<br><br>To move an engagement into the **Validate** state, click **Validate** on any engagement currently in the **Scope** state. |
| Fieldwork | Auditors complete their assigned audit tasks during the **Fieldwork** state. These tasks include control testing, interviews, walkthroughs, and other activities. Issues that are found during control testing are associated with the engagement. Auditors can also create general issues associated with the engagement. Audit managers can create additional audit tasks as needed. When the audit is done, audit managers specify the result of the engagement, whether it's satisfactory, adequate or inadequate, and provide details on their opinion.<br><br>To move an engagement into the **Fieldwork** state, click **Advance to Fieldwork** on any engagement currently in the **Validate** state.<br><br>See Audit task management. |
| Awaiting Approval | During the "Awaiting Approval" state, the approvers specified in the **Approvers** field of the engagement review the results of the audit tasks conducted and the issues that were created. After reviewing the results of the engagements, approvers approve or reject the engagement.<br><br>To move an engagement into the **Awaiting Approval** state, click **Request approval** on any engagement currently in the **Fieldwork** state.<br><br>See Approve or reject an engagement. |
| Follow Up | After an engagement has been approved, if there are any remaining open tasks, issues or milestones, in case of GRC Advanced Audit, associated with the engagement, the engagement automatically goes into the **Follow Up** state. During this stage, auditors must close out all remaining issues, tasks, and milestones before the engagement are marked as complete. |
| Closed | Engagements move into the "Closed" state under one of three conditions: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States of the engagement process (continued)**

| State | Description |
|---|---|
| | • The engagement is closed as incomplete during the **Scope**, **Validate**, or **Fieldwork** states.<br>• There are no open audit tasks, issues, and milestones after the engagement is approved. In this case, the engagement automatically moves from the **Awaiting Approval** state to the **Closed** state.<br>• All follow-up tasks, issues, and milestones are closed out. In this case, the engagement automatically moves from the **Follow Up** state to the **Closed** state. |

### Audit task management

Audit tasks are completed throughout an engagement and provide documented evidence that the organization is complying with external regulations and internal policies.

When audit tasks are created or reassigned, a notification is sent to the assigned user. A notification is also sent when the task reaches 75% of its planned duration.

### Create an engagement

Audit managers create engagements to manage audit information and collect entities, controls, and control tests that are relevant to the audit.

#### Before you begin

Role required: sn_audit.admin or sn_audit.manager

#### About this task

To know more about how to define a control and control objective, see:

- Create a control
- Create a control objective

#### Procedure

1. Navigate to **All** > **Audit** > **Engagements** > **Create New**.
2. On the form, fill in the fields.

**Engagement form**

| Field | Description |
|---|---|
| Number | A unique identification number. |
| State | ◦ Scope<br>◦ Validate and plan<br>◦ Fieldwork<br>◦ Awaiting approval<br>◦ Follow up<br>◦ Closed |
| Name | Name of the engagement. |
| Type | Type of engagement. The choices are: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ None<br>◦ Internal Audit<br>◦ External Audit<br>◦ SOX Audit<br>◦ IT Audit<br>◦ Financial Audit<br>◦ Compliance Audit<br>◦ Certification Audit<br>◦ Regulatory Audit<br>◦ Operational Audit<br>◦ Continuous Audit<br>◦ Vendor Audit<br>◦ Customer Audit<br>◦ Store Audit<br>◦ Quality Audit<br>◦ Project Audit |
| Percent complete | Number that represents the percentage of the engagement that has been completed. |
| Assigned to | User assigned to the engagement. |
| Auditors | Auditors assigned to the engagement. |
| Approvers | Approvers assigned to the engagement. |
| Description | General description of the engagement. |
| Objectives | Stated objectives of the engagement. |
| Schedule | |
| Engagement planned start | Estimated start date of the engagement. |
| Engagement starts | Choice to automatically determine the start date of the engagement. The choices are:<br>◦ Scope<br>◦ Validate<br>◦ Fieldwork |
| Engagement actual start | Actual date the engagement begins. |
| Engagement planned end | Estimated end date of the engagement. |
| Engagement ends | Choice to automatically determine the start date of the engagement. The choices are: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ Follow Up<br>◦ Closed |
| Engagement actual end | Actual date the engagement ends. |
| Fieldwork planned start | Estimated start date of the fieldwork. |
| Fieldwork planned end | A planned end date that was originally set in the engagement.<br>**Note:** This field sets the value as one day plus the planned start date for fieldwork by default. |
| Fieldwork planned duration | Number of days and hours planned for fieldwork. The duration and planned start date of fieldwork are used to calculate the planned end date. If audit tasks are defined, this field is populated with the longest planned duration from the audit tasks. |
| Fieldwork actual start | Actual start date of the fieldwork. If audit tasks are defined, this field is populated with the earliest actual start date from the audit tasks. |
| Fieldwork actual end | Actual end date of the fieldwork. If audit tasks are defined, this field is populated with the latest actual end date from the audit tasks. |
| Fieldwork actual duration | Duration of fieldwork start date and end date. |
| Results | |
| Result | ◦ Satisfactory<br>◦ Adequate<br>◦ Inadequate |
| Opinion | Justification for the selected result. |
| Report | |
| Knowledge base | Knowledge base to be used. |
| Report template | Template to be used to generate the knowledge base article reporting the engagement results. |
| KB article | Recently generated knowledge base article containing the engagement results |
| Activity | |
| Additional comments | Customer-viewable comments. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Work notes | Comments that are viewable by the admin and audit manager. |
| Confidentiality | |
| Confidential | Option to enable the confidentiality of the record. Only the assigned users or groups of users can access the record.<br><br>For more information on the confidential option, see Confidentiality flag for audit and compliance records. |

3. Select **Submit**.

### Generate an audit report from an engagement

Generate an audit report and maintain different versions of audit reports from an engagement in Follow up state.

#### Before you begin
Role required: sn_audit.manager

#### About this task
When an engagement is in the **Follow up** state, the audit lead can generate an audit report. An audit report is represented in the form of a knowledge base (KB) article. After an audit report is generated, an incremented version of the report is created instead of a new report or KB article. After you make major changes to an audit report and publish the report, a new major version of the report is created.

#### Procedure
1. Navigate to **All** > **Audit** > **Engagements** > **All Engagements**.
2. Open the engagement for which you want to generate an audit report.
3. Click the **Report** tab.
   a. In the **Knowledge base** field, select the knowledge base.
   b. In the **Report template** field, select the template.
4. Click **Generate report**.
5. To publish the KB article without making any changes, click **Publish**
6. To edit the KB article, click **Edit.**.
   The KB article page appears with the state of the KB article as **Draft** and a minor version of the article is created.
7. Edit the KB article as necessary and click **Publish**.

#### Result
The incremented version of the report appears in the **KB article**field in the **Report** tab.

### Create an engagement from a previous engagement

Audit managers can create engagements from previous engagements to reduce the need to redefine the scope, auditors, and approvers for similar engagements that are conducted throughout the year.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_audit.admin or sn_audit.manager

### Procedure
1. Navigate to **All** > **Audit** > **Engagement** > **All Engagements**.
2. If necessary, clear the search filter criteria.
3. Open the engagement to copy from.
4. Right-click the header of the engagement and click **Copy Engagement**.

## Create a control test from an engagement

After defining a control, audit managers create control tests that run periodically and provide documented evidence of whether the associated control is operating correctly.

### Before you begin
Role required: sn_audit.admin and sn_audit.manager

### Procedure
1. Navigate to **All** > **Audit** > **Engagements** > **All Engagements**.
2. Open the engagement for the audit task you want to create.
   Assign audit tasks to engagement in one of the following states:
   - Validate
   - Fieldwork
   - Awaiting approval
3. In the **Audit Tasks** Related List, click **New**.
4. In the Audit Tasks Interceptor, click **Control Test**.
5. On the form, fill in the fields.

**Control test form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| State | ◦ Open<br>◦ Work in Progress<br>◦ Review<br>◦ Closed Complete<br>◦ Closed Incomplete<br>◦ Closed Skipped |
| Parent | Parent audit task. |
| Control effectiveness | Control effectiveness. |
| Assigned to | User assigned to this control test. |
| Issue | Issue related to this control test. |
| Test plan | Test plan associated with this control test. |
| Short description | Brief description of the control test. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Schedule | |
| Planned start date | Intended date the control test should begin. |
| Planned end date | Intended date the control test should end. |
| Planned duration | Expected duration of this control test. As with actual duration, the planned duration shows total activity time and takes the control test schedule into consideration. |
| Actual start date | Date that this control test began. |
| Actual end date | Date that this control test ended. |
| Actual duration | Duration of the control test from control test start to control test closure. |
| Design test | |
| Design effectiveness | ◦ Effective<br>◦ Ineffective |
| Design expectations | Basic requirement that should be met by a control so that it is effective. This checks if the control was designed properly to achieve the control objective. |
| Design assessment procedures | Procedure or steps to be followed to conclude whether the design of the control is effective to achieve the control objective or not. This is based on the design expectation. |
| Design results | Results of testing the design of the control based on the design assessment procedure. |
| Operation test | |
| Operation effectiveness | ◦ Effective<br>◦ Ineffective |
| Operation expectations | Expectations that should be met to ensure that the control is operating effectively to achieve the control objective. |
| Operation assessment procedures | Detailed steps, to carry out the operation expectations, which need to be performed to conclude that the control is operating successfully. |
| Operation results | Results of testing the operation of the control based on the operation assessment procedure. |
| Activity journal | |
| Work notes | Comments that are viewable by the audit manager. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Additional comments | Customer-viewable comments. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |

6. Click **Submit**.

### Automatically generate control tests from an engagement

After adding an entity to an engagement, you can automatically generate control tests.

#### Before you begin
Role required: sn_audit.admin and sn_audit.manager

#### Procedure
1. Navigate to **All** > **Audit** > **Engagements** > **All Engagements**.
2. Open the engagement for which you want to generate control tests.
3. Click the Test Plans related list.
4. Select the test plans for which you want to generate control tests.
5. Click **Generate Control Tests**.

#### Result
The controls tests for each test plan is created under the Audit Task related list.

### Create an audit task activity

After defining a control, audit managers create activities that explore and provide documented evidence of whether the associated control is operating correctly.

#### Before you begin
Role required: sn_audit.admin and sn_audit.manager

#### Procedure
1. Navigate to **All** > **Audit** > **Engagements** > **All Engagements**.
2. Open the engagement for the audit task you want to create.
   Assign audit tasks to engagement in one of the following states:
   - Validate
   - Fieldwork
   - Awaiting approval
3. In the **Audit Tasks** related list, click **New**.
4. In the Audit Tasks Interceptor, click **Activity**.
5. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Activity form

| Field | Description |
|---|---|
| Number | Unique identification number. |
| State | ◦ Open<br>◦ Work in Progress<br>◦ Review<br>◦ Closed Complete<br>◦ Closed Incomplete<br>◦ Closed Skipped |
| Parent | Parent audit task. |
| Assigned to | User assigned to this activity. |
| Short description | Brief description of the activity. |
| Description | Detailed explanation of the activity. |
| Schedule | |
| Planned start date | Intended date the activity should begin. |
| Planned end date | Intended date the activity should end. |
| Planned duration | Expected duration of this activity. As with actual duration, the planned duration shows total activity time and takes the activity schedule into consideration. |
| Actual start date | Date that this activity began. |
| Actual end date | Date that this activity ended. |
| Actual duration | Actual duration of the project from project start to project closure. |
| Activity | |
| Additional comments | Customer-viewable comments. |
| Work notes | Comments that are viewable by the audit manager and audit manager. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |

6. Click **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create an interview

After defining a control, audit managers create interviews with control owners to discuss and provide documented evidence of whether the associated control is operating correctly.

**Before you begin**
Role required: sn_audit.admin and sn_audit.manager

**Procedure**

1. Navigate to **All** > **Audit** > **Engagements** > **All Engagements**.
2. Open the engagement for the audit task you want to create.
   Assign audit tasks to engagement in one of the following states:
   - Validate
   - Fieldwork
   - Awaiting approval
3. In the **Audit Tasks** Related List, click **New**.
4. In the Audit Tasks Interceptor, click **Interview**.
5. On the form, fill in the fields.

**Interview form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| State | ◦ Open<br>◦ Work in Progress<br>◦ Review<br>◦ Closed Complete<br>◦ Closed Incomplete<br>◦ Closed Skipped |
| Parent | Parent audit task. |
| Assigned to | User assigned to this interview. |
| Short description | Brief description of the interview. |
| Description | Detailed explanation of the interview. |
| Schedule | |
| Planned start date | Intended date the interview should begin. |
| Planned end date | Intended date the interview should end. |
| Planned duration | Expected duration of this interview. As with actual duration, the planned duration shows total activity time and takes the interview schedule into consideration. |
| Actual start date | Date that this interview began. |
| Actual end date | Date that this interview ended. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Actual duration | Duration of the interview from interview start to interview end. |
| Assignment | |
| Primary Contact | User to contact for this interview. |
| Other Contacts | Other users to contact for this interview, if the primary contact is unavailable. |
| Notes | Additional notes about the interview contacts. |
| Activity | |
| Additional comments | Customer-viewable comments. |
| Work notes | Comments that are viewable by the audit administrator and audit manager. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |

6. Click **Submit**.

### Create a walkthrough

After defining a control, audit managers create walk throughs that will be conducted to observe and provide documented evidence of whether the associated control is operating correctly.

## Before you begin

Role required: sn_audit.admin and sn_audit.manager

## Procedure

1. Navigate to **All** > **Audit** > **Engagements** > **All Engagements**.
2. Open the engagement for the audit task you want to create.
   Assign audit tasks to engagement in one of the following states:
   - Validate
   - Fieldwork
   - Awaiting approval
3. In the **Audit Tasks** Related List, click **New**.
4. In the Audit Tasks Interceptor, click **Walkthrough**.
5. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Walkthrough form

| Field | Description |
|---|---|
| Number | Unique identification number. |
| State | ◦ Open<br>◦ Work in Progress<br>◦ Review<br>◦ Closed Complete<br>◦ Closed Incomplete<br>◦ Closed Skipped |
| Parent | Parent audit task. |
| Assigned to | User assigned to this walkthrough. |
| Short description | Brief description of the walkthrough. |
| Description | Detailed explanation of the walkthrough. |
| Schedule | |
| Planned start date | Intended date the walkthrough should begin. |
| Planned end date | Intended date the walkthrough should end. |
| Planned duration | Expected duration of this walkthrough. As with actual duration, the planned duration shows total activity time and takes the walkthrough schedule into consideration. |
| Actual start date | Date that this walkthrough began. |
| Actual end date | Date that this walkthrough ended. |
| Actual duration | Duration of the walkthrough from start to end. |
| Walkthrough | |
| Primary Contact | User to contact for this walkthrough. |
| Other Contacts | Other users to contact for this walkthrough, if the primary contact is unavailable. |
| Execution Steps | Detail the activities to be performed during the walkthrough. |
| Explanation | Intended purpose of the walkthrough. |
| Additional Information | Additional information the user conducting the walkthrough needs to be aware of. |
| Results | Details of what transpired during the walkthrough. |
| Activity | |
| Additional comments | Customer-viewable comments. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Work notes | Comments that are viewable by the audit manager and audit manager. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |

6. Click **Submit**.

### Generate a KB article from an engagement

Audit managers can generate a KB article that summarizes the findings of an engagement so report findings can be communicated to executives.

#### Before you begin

Role required: sn_audit_manager
KB articles can be generated for engagements in the **Awaiting approval**, **Follow up**, and **Closed complete** states.

#### Procedure

1. Navigate to **All** > **Audit** > **All Engagements**.
2. Open the engagement record.
3. Fill in the fields on the **Reports** tab, as appropriate.

**Reports tab on engagement form**

| Field | Description |
|---|---|
| Report template | Select the report template to use for this KB article. |
| KB article | Read-only field that is automatically populated with a unique identification number. |

4. Click **Generate report**.

### Approve or reject an engagement

Audit users that are assigned as approvers for an engagement can approve or reject engagements in the **Awaiting Approval** state.

#### Before you begin

Role required: sn_audit.user

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Audit** > **My Audit Approvals**.
2. Open the approval record associated with the engagement.
3. Click **Approve** or **Reject**
   One of the following actions occurs:
   - If the engagement is approved and there are remaining open tasks or issues, it automatically moves into the **Follow Up** state.
   - If the engagement is approved and there are no remaining open tasks or issues, it automatically moves into the **Closed** state.
   - If the engagement is rejected, it automatically moves back to the **Fieldwork** state

#### Add entities to an engagement scope

Audit managers can define which entities are involved in the audit engagement. When you add an entity to an engagement, the corresponding risks, controls, test plans, and indicator results of the entity are also added to the engagement.

### Before you begin

Role required: sn_audit.manager or sn_audit.admin

### Procedure

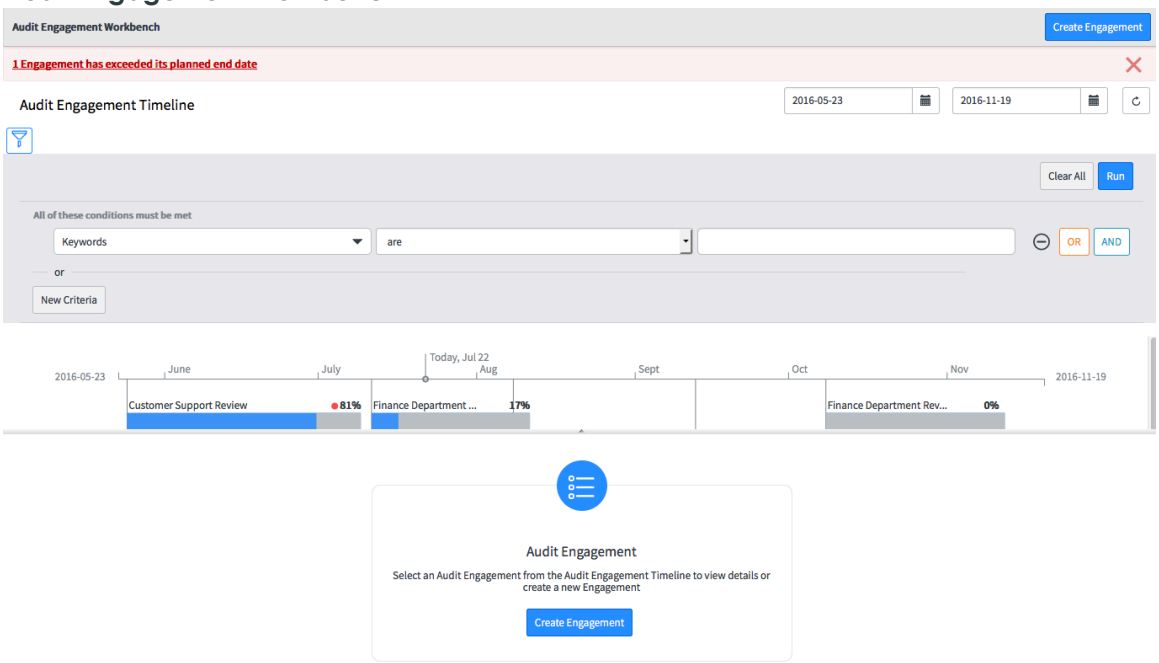
1. Navigate to **All** > **Audit** > **Engagements** > **All Engagements**.
2. Open an engagement in the **Scope** state.
3. In the **Entities** related list, click **Add**.
4. Select the desired entities that are included in the audit engagement.
5. Click **Add**.
   If there are risks and controls, test plans, and indicator results associated with an entity then they appear in their respective sections.

#### Use the Audit Engagement Workbench to visually manage engagements

The Engagement Workbench provides a timeline view from which you can select an audit engagement to view details or create a new engagement.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Audit Engagement Workbench




### Create an engagement from Audit Workbench

The Engagement Workbench provides a timeline view from which you can select an audit engagement to view details or create a new engagement. Audit managers create engagements directly from the Workbench to manage audit information and collect entities, controls, and control tests that are relevant to the audit.

### Before you begin

Role required: sn_audit.admin or sn_audit.manager

### Procedure

1. Navigate to **All** > **Audit** > **Engagements** > **Workbench**.
2. Click **Create Engagement**.
3. On the form, fill in the fields.

#### Engagement form

| Field | Description |
|---|---|
| Name | Name of the engagement. |
| Assigned to | User assigned to the engagement. |
| Description | General description of the engagement. |
| Objectives | Objectives of the engagement. |
| Planned start date | Intended date the activity should begin. |
| Planned duration | Expected duration of this activity. As with actual duration, the planned duration shows total activity time and takes the activity schedule into consideration. |
| Audit period start | Date that work on the engagement is expected to begin. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Audit period end | Date that work on the engagement is expected to end. |
| Auditors | Auditors assigned to the engagement. |
| Approvers | Approvers assigned to the engagement. |

4. Click **Create**.

## Manage your documents and work papers with Audit Management as cloud files

You can manage your documents and work papers with Audit Management as cloud files. The document integration with the cloud files providers functionality enables you to establish a connection between the cloud files providers such as Microsoft OneDrive and ServiceNow®. You can then manage documents and work papers as cloud files in Microsoft OneDrive instead of attaching them to the record.

Beginning with the Utah release, the document integration functionality is supported on the engagement and audit task records. This capability addresses specific use cases for the engagement and audit task records in the Audit Workspace.

## Key benefits of workpapers and document management using Microsoft OneDrive

The document integration functionality provides the following benefits for the users:

- Connect to the existing documents on Microsoft OneDrive such as Excel, Microsoft PowerPoint presentations, and Microsoft Word documents etc.
- Mark a document as confidential.
- Share the non-confidential documents between different GRC records.
- Control read and write access to the cloud files based on the configurable permissions.
- Collaborate on the workpapers using the Microsoft OneDrive capability.

## Use cases for managing the cloud files

The document integration functionality addresses the following use cases for the customers:

- Edit and read the documents and workpapers using Microsoft OneDrive based on the configured access.
- Connect to the existing documents and workpapers on Microsoft OneDrive.
- Reference and link the cloud files that are already connected to other GRC records.
- Configure the cloud file conditions in the Cloud file configuration record. Based on the configured conditions, the action buttons to add, remove, reference, and link the file are displayed in the **Cloud files** related list.
- Mark a file that cannot be shared between the records as confidential or the corresponding cloud file on Microsoft OneDrive cannot be connected to any record.
- Configure the cloud file access to provide read and write access to the users based on the defined conditions.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Roles required to manage the document integration tasks

The following roles are required to manage the document integration tasks.

**Roles required and corresponding tasks**

| Roles | Tasks |
|---|---|
| Auditor (sn_audit_ws.auditor) and Audit Supervisor (sn_audit_ws.supervisor) | Can perform the following tasks:<br>• Connect to the existing documents and workpapers on Microsoft OneDrive.<br>• Edit and read the documents and workpapers using Microsoft OneDrive based on the configured access.<br>• Reference and link the cloud files that are already connected to other GRC records.<br>• Mark a file as confidential. |
| Workspace Admin (sn_grc_workspace.admin) | Can configure the cloud file access to provide read and write access to the users based on the defined conditions. |

**Note:** For general guidelines on managing the documents using Microsoft Office 365, see KB1587297.

### Complete the prerequisites to manage your documents using Microsoft OneDrive

Complete the prerequisites to manage your documents using Microsoft OneDrive so that you can enable the cloud file integration.

**Before you begin**
Role required: sn_grc_workspace.admin

**About this task**
Ensure that you have installed the following applications:

- Document Management (com.snc.platform_document_management)
- Microsoft OneDrive Spoke for Document Service Framework (sn_docs_onedrive)

**Note:** Integration Hub entitlements included in the Audit Workspace are solely restricted to the use for Microsoft OneDrive integration. All other use requires the applicable purchase of an additional Integration Hub entitlement.

**Procedure**

1. Set up the Microsoft OneDrive Integration Hub Spoke.

   Set up the Microsoft OneDrive connection to perform actions in Microsoft OneDrive from ServiceNow.

   - For grant type as *Authorization Code*, use a service account to generate the *OAuth* token. All the file operations in Microsoft OneDrive from ServiceNow are executed using this service account. The end user must ensure that the service account is also the owner of the file that the user is trying to link with the file.

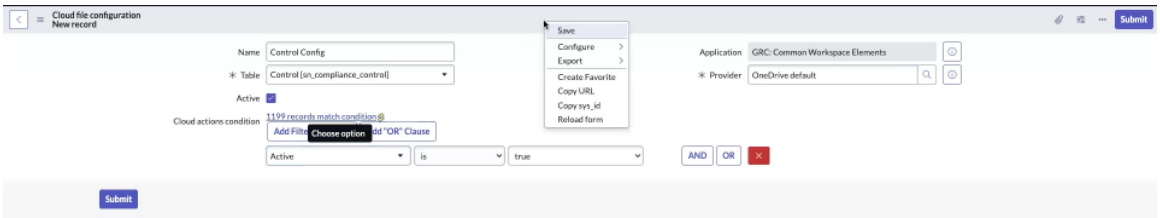
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The required API permissions in Azure application registration are *openid*, *email*, *Files.Read*, *Files.ReadWrite.All*, *offline_access*, *User.Read*, *User.ReadBasic.All*.

- For grant type as *Client Credentials*, the required API permissions in Azure application registration are *Files.Read.All* and *Files.ReadWrite.All*.

2. Navigate to **Policy and Compliance** > **Administration** > **GRC properties** and select **One drive** in the *Select a file sharing service to host documents and attachments* property.
3. Navigate to the **Cloud file configurations** module and configure this feature for Engagement and Audit tasks.

   The Cloud file configuration record is displayed.




For more information on the fields, see Create a Cloud file configuration record.

### Create a Cloud file configuration on engagements and audit tasks

The GRC Workspace administrators can create a Cloud file configuration on engagements and audit tasks and manage access permissions on the cloud files.

Beginning with the Utah release, the Cloud file configuration module is used to create a cloud configuration record and manage the access permissions on the attached cloud files.

## Roles required to access the Cloud file configuration module

Workspace users with the following roles can access the Cloud file configuration module:

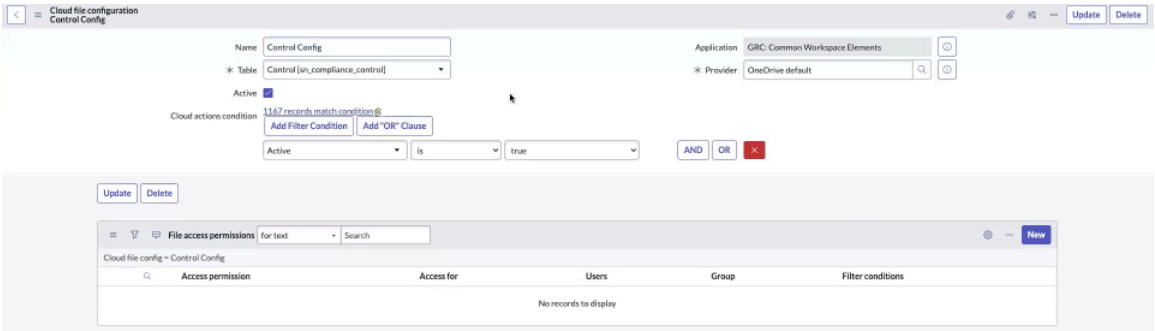
**Roles**

| Role | Permissions |
|---|---|
| Workspace administrator [sn_grc_workspace.admin] | CRUD permissions |
| Workspace user [sn_grc_workspace.user] | Read permissions |

## Cloud file configuration module

If you are the Workspace administrator with the sn_grc_workspace.admin role, you can update the following fields in the Cloud file configuration module to configure the permissions as shown in the example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




- Name: Name of the document access record. For example, Engagement document access.
- Table: Table that is used for the document access record. For example, Engagement [sn_audit_engagement].
- Active flag: Flag to mark the cloud file configuration as active.
- Provider: Provider for the document access record. The default option for this field is Microsoft OneDrive.
- Cloud action condition: Filter conditions for the cloud files. Based on the configured conditions, the action buttons are rendered in the Cloud files related list.

### Create a Cloud file configuration record

Create a cloud file configuration record to manage the access permissions on the cloud document.

#### Before you begin

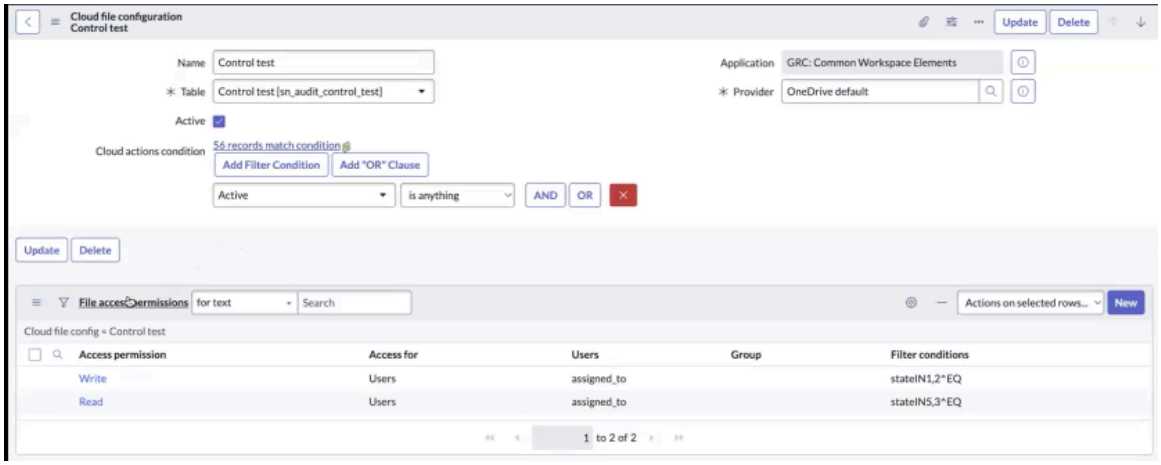
Role required: sn_grc_workspace.admin (CRUD), sn_grc_workspace.user (Read)

#### Procedure

1. Navigate to **All** > **GRC Administration** > **Cloud file configuration**.
2. Select **New**.
   The Cloud file configuration record is displayed.
3. On the Cloud file configuration form, fill in the fields.

   For more information on the fields in the form, see Cloud file configuration record form.
   Once the parent cloud file configuration is active, you can configure the File access permissions for the Cloud file configuration record as shown in the example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




4. Select **Update**.

### Cloud file configuration record form

Update the access permissions for a record in the Cloud file configuration record form.

## Cloud file configuration record form

For a description of the field values, see the following table.

**Cloud file configuration record form**

| Field | Description |
|---|---|
| Name | Name of the Cloud file configuration record. For example, Engagement document access. |
| Table | Table used for the Cloud file configuration record. For example, Engagement [sn_audit_engagement]. For all the files used in this table, the access permissions are configured in this form. |
| Active | Option to mark the record as active. |
| Provider | Provider for the Cloud file configuration. Location where the files are present in the cloud. The default option is **OneDrive default**. |
| File access permissions | |
| Access permission | Read or Write permission for the record. |
| Access for | Users or groups for which the cloud file access is configured. |
| Users | Selected users for which an access to the cloud files will be provided. |
| Group | Selected group of users for which an access to the cloud files will be provided. |
| Filter condition | Condition used to create the document access record. A sample condition would |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Cloud file configuration record form (continued)**

| Field | Description |
|---|---|
| | be: "**State**" "**is one of**" "**Open**, **Work In Progress**, **Review**." |

### Create a File access permission record to manage the permissions

Create a File access permission record and manage the access permissions on the cloud document.

### Before you begin

Role required: sn_grc_workspace.admin (CRUD), sn_grc_workspace.user (Read)

### About this task

By default, the file access permissions are enabled on the engagement and audit task records. A user that is part of a group can select **Request access** to request an access to the file. The **Request access** UI action is available only to the group members. A user that is part of a cloud file configuration can use **Refresh file access** to refresh or configure the file access. The **Refresh file access** action is available to the users that are listed in the cloud file configuration.

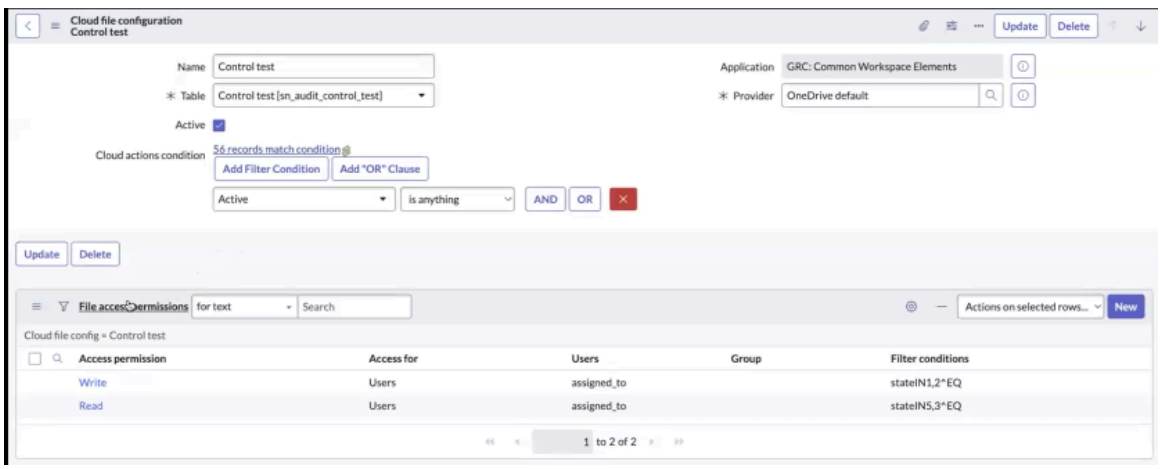
Instead of using the manual **Request access** and **Refresh file access** actions, you can configure file access permissions on other tables such as control records or policy records. For more information, see the configuration steps in KB1587297.

### About this task

The File access permission record enables the users to manage access permissions on the cloud document.

### Procedure

1. Navigate to **All** > **GRC Administration** > **Cloud file configuration**.
2. Select an active parent cloud file configuration record.
   The cloud file configuration record is displayed.

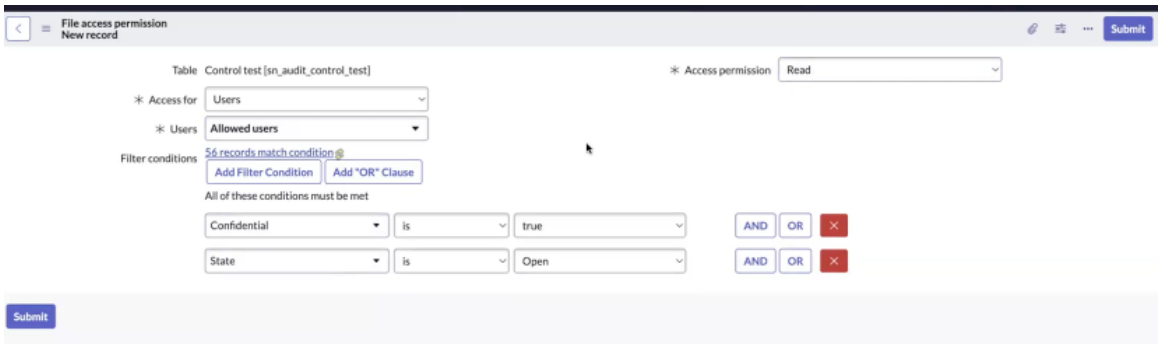



3. In the File access permissions related list, select **New**.

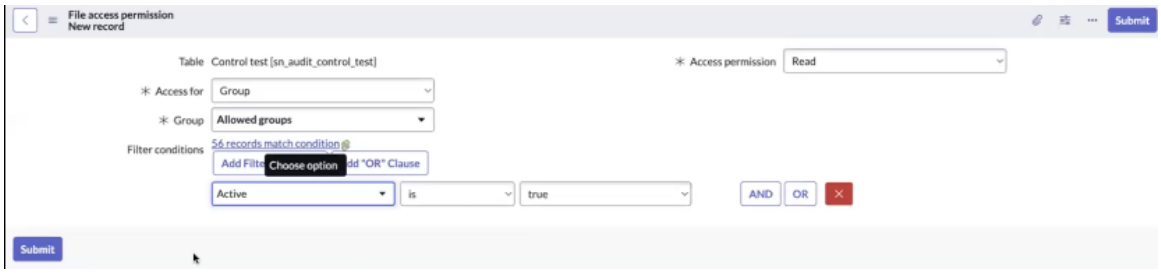
   You can use the **Users** field to select one of the user (sys_user) fields from an engagement or audit task such as engagement lead, auditors, and so on. The users selected in the **Users** field are granted access to the cloud file.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can configure the file access permissions for one or more users of the record as shown in the following example.




You can use the **Group** field on the form to select one of the group (sys_user_group) fields from an engagement or audit task such as an assignment group. The users that are part of the group are granted access to the cloud file. A File access group permission record is displayed in the following example.




4. On the form, fill in the fields.
   For more information on the fields in the form, see File access permission record form.
5. Select **Submit**.
   Based on the configuration set up in the form, the permissions on the cloud document are evaluated.

### File access permission record form

Update the File access permission record form for a Cloud file.

## File access permission record form

For a description of the field values, see the following table.

**File access permission record form**

| Field | Description |
|---|---|
| Table | Name of the table for which the access permissions are configured. For example, Control Test [sn_audit_control_test]. |
| Access for | Access for the users or a group. For example, Engagement [sn_audit_engagement]. For all the files used in this table, the access permissions are configured in this form. |
| Users | Access permissions that can be configured for the users. Displays a tree structure of |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**File access permission record form (continued)**

| Field | Description |
|---|---|
| | all the user fields for the selected record. When the permissions are refreshed, they're automatically refreshed and assigned to the users. |
| Group | Access permissions that can be configured for the users of a group. Displays a tree structure of all the group fields for the selected record. When the permissions are refreshed for the first time, every group member in the group who wants to have access to the document, should select the engagement record and select the **Request access** action manually to access the document.<br><br>The users of a group do not automatically receive an access to the record for the first time. They must request an access for the first time.<br><br>For the subsequent operations on the record, access for the users (who requested it for the first time) is also refreshed. |
| Access permission | Type of access permission to be configured for the selected user. For example, Read or Write. |
| Filter condition | Condition that describes when the file access permissions are applied. |

### File access permissions

The Workspace administrators with the sn_grc_workspace.admin role can configure the file access permissions for the users and groups.

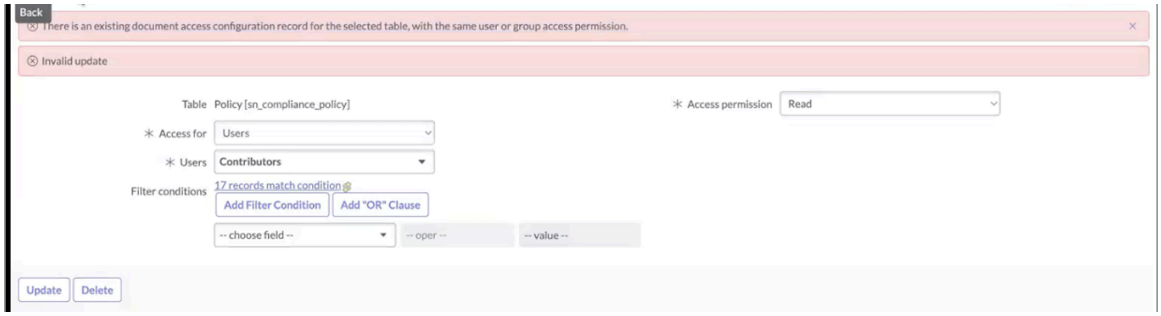
## Conditions for file access permissions

The Workspace administrators with the sn_grc_workspace.admin role can configure different conditions for file access permissions:

- For a combination of the **Table** field, **Access permission** field, and **Users** field, you can have only one File access permission record. If you have an existing record for a table with a given set of user and access permissions, you cannot create a duplicate record with the same access permissions. For example, if a contributor has Read access permission for the policy (sn_compliance_policy) record, creating another record for the same condition is not permitted.

- For a given combination of the **Table** field, **Provider** field, and **Active** option, only one Cloud file configuration record is permitted. A duplicate configuration is not permitted for an active table as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




- If a user is part of multiple **User** fields or a **Group** field, a higher access is granted to the user.

## Source link and reference link to the GRC record

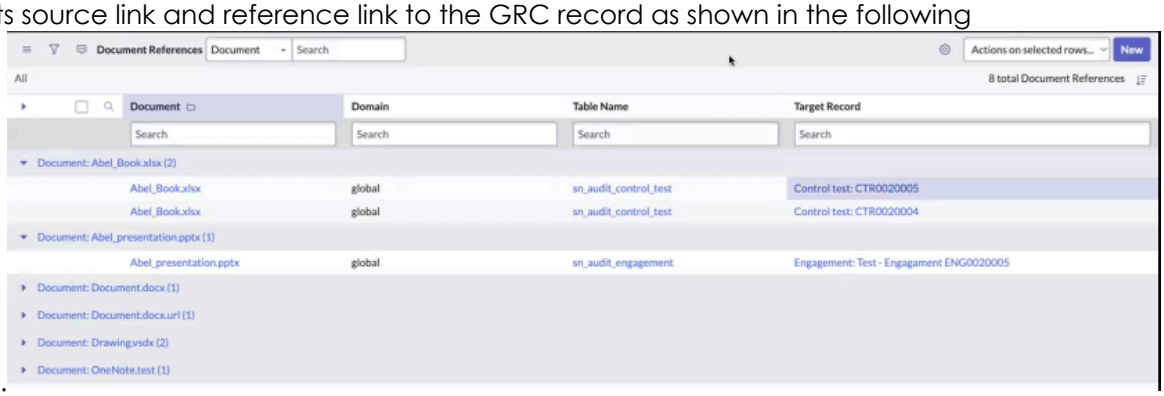
When a cloud file is connected to a GRC record for the first time, the connection is considered as a source link to the GRC record.

When the same cloud file is mapped to another GRC record, then it is considered as a reference link to the GRC record.

A source link to the GRC record always has the write access and the reference link to the GRC record always has the read access.

When a record is mapped as a source link to the cloud file, the configuration is applied as it is to the cloud file. For example, if the configuration contains write access for some users and read access for some users, the same configuration is maintained and applied to the users.

The Document reference table shows how one document record is being referenced such as its source link and reference link to the GRC record as shown in the following example.




Consider the example of Engagement_memo.xslx for which Control test CTR0020005 is a source link and Control test CTR0020004 is a reference link. For any configuration that matches the configuration of Control test CTR0020004, all the users under this configuration even though they have Write access in the configuration has only read access.

Consider the following example where a Risk and Controls Matrix Report is connected to Engagement record 1 and Engagement record 2.

### Example: Access document and the associated records

| Document | Record that the document is connected to |
|---|---|
| Risk and Controls Matrix Report | Engagement record 1. It is the source for the access document. |
| Risk and Controls Matrix Report | Engagement record 2. It is the reference for the access document. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

See the following table for the permissions assigned for the example.

**Example: Assigned access permissions**

| Access doc connected to the record | Users field value | Type of access | Description |
|---|---|---|---|
| Engagement record 1 | Contributors | Have Write access | For the source record, the permission configuration is considered as it is configured. Therefore, the contributors have the Write access to Engagement 1. |
| Engagement record 2 | Reviewers | Have Write access | The same access record is mapped to Engagement 2, for which the reviewers should have the Write access. Because Engagement record 2 is a reference record, the reviewers have the Read access instead of the Write access. |

## Another use case for source link

When the cloud document is mapped to a record, it becomes a source link for the cloud document. If the same record is removed and the cloud document is mapped to another GRC record, the next record becomes the source link for the cloud document.

For example, the Engagement_memo.xlsx file is mapped to the engagement 1 and engagement 2 records. The engagement 1 record is the source link and the engagement 2 record is the reference link. If the mapping between the Engagement_memo.xlsx file and the engagement 1 record is removed, the Engagement_memo.xlsx file does not have any source link. If the Engagement_memo.xlsx file is mapped to the engagement 3 record, then the engagement 3 record becomes the source link for the document.

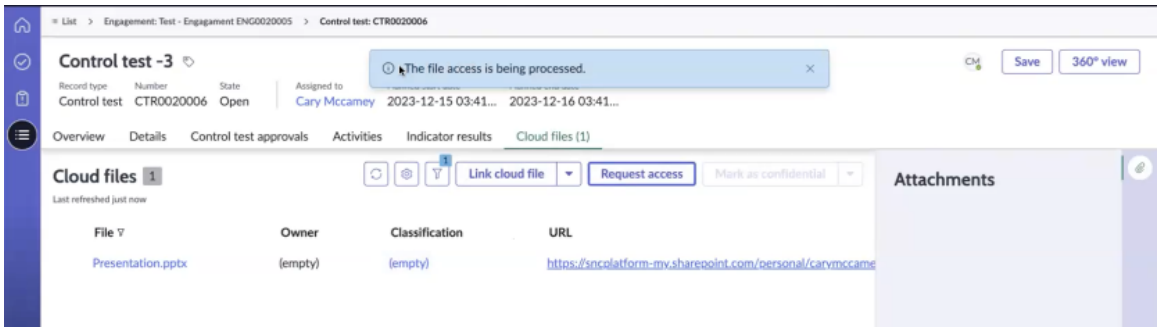
## Request access and Refresh file access actions

By default, the file access permissions are enabled on the engagement and audit task records. For other records, you can use the **Request access** and **Refresh file access** actions on the form. By default, the file access permissions are enabled on the engagement and audit task records. If a user is part of a group, they can use the **Request access** UI action to request access to the file. The **Request access** UI action is available only to the group members. If the user is part of a cloud file configuration, they can use the **Refresh file access** action to refresh or configure the file access. The **Refresh file access** action is available to the users mentioned in the cloud file configuration.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To configure the file access permissions on other tables such as control records or policy records (instead of using the manual **Request access** and **Refresh file access** actions), see the configuration steps in KB1587297.

The users that are part of a group should request access to the cloud file by using the **Request access** action button. When a user who is part of the Audit Managers group selects **Request access** on the form, a UI message is displayed as shown in the example: `The file access is being processed.`




Requesting access to the cloud file is a one-time activity for the users of a group. If a user selects **Request access** more than once and the access has already been granted, the following message is displayed: `File access has already been granted.`

If the user requests access to the cloud file and if the request is not processed in time, an error message is displayed on the screen. The user must select **Refresh file access** to request an access to the file again.

### Connect to a cloud file

Connect to a cloud file on Microsoft OneDrive with file path and file name. You can then link the cloud file to a record in the Workspace.

### Before you begin

Role required: sn_audit_ws.auditor, sn_audit_ws.supervisor

Ensure that the cloud file UI actions on the Cloud files related list are visible on the forms based on the configured conditions. Ensure that file access permissions of read and write are added for the auditor and engagement leads. For more information, see Create a Cloud file configuration on engagements and audit tasks.

### About this task

Beginning with the Utah release, cloud file integration is enabled on the engagement and audit task records using the Microsoft OneDrive integration. Therefore, this task refers to linking a cloud file from Microsoft OneDrive to an engagement record.

### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the tasks icon ( ).
   The list displays the engagements that are assigned to you.
3. Create an audit engagement or navigate to an existing engagement and go to the **Cloud files** tab.
4. In the **Cloud files** tab, select **Link cloud file**.
   The Add file pop-up is displayed.
5. In the **File location** field, enter the path of the folder where the file resides on Microsoft OneDrive.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The valid characters for the folder location are [a-z], [A-Z], [0-9], [_], [-], [/].

6. In the **File name** field, enter the name of the file with the file format.
   The valid characters for the file name are [a-z], [A-Z], [0-9], [()], [_], [-], [.] [space]. The file name should also include the file extension such as .docx, .ppt, .xls.
7. Select the **Mark as confidential** option.

   When this option is selected, the cloud file that is linked to the record is marked as confidential. When a file is marked as confidential, it cannot be shared with other records in ServiceNow. If you attempt to link a confidential file to another ServiceNow record, the following error message is displayed: `The file cannot be added to the record as it is confidential`. When the file is marked as non-confidential, the cloud file can be linked to another record.

   **Note:**

   Integration Hub entitlements included in the Audit Workspace are for Microsoft OneDrive integration. Using Microsoft OneDrive integration requires Integration Hub transactions not included in the Audit Workspace product, but requires an Automation Engine or Integration Hub subscription.

8. Select **Link** in the pop-up.
   When the cloud file is linked to a record, the file access permissions are refreshed according to the set permissions on the table. For information on File access permissions, see Create a Cloud file configuration on engagements and audit tasks.
   The cloud file is linked to the record. The following UI message is displayed: `The file is linked successfully`. The cloud file is then displayed in the Cloud files related list on the record form.

   Once the file is connected on Microsoft OneDrive, the auditor or engagement lead gets read or write access based on the defined access permissions.

### Link a reference cloud file

Link a reference cloud file that is already associated to other GRC records. You can link non-confidential files only.

#### Before you begin

Role required: sn_audit.admin, sn_audit.manager, sn_grc_workspace.user

#### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the tasks icon (  ).
3. Create a new audit engagement or navigate to an existing engagement and go to the **Cloud files** tab.
   The list displays the engagements that are assigned to the logged-in user.
4. In the **Cloud files** tab, select **Link reference file**.
   The Link reference file pop-up is displayed.
5. In the **Select file** field, select the reference file that you want to link to the record.

   The field populates the cloud files that are classified as Public.

   **Note:** You cannot link a confidential document as a reference file with other records. The files that are marked as confidential are not displayed in the list of available files in the pop-up.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Select **Link** in the pop-up.
   When a cloud file is linked to a record, the file access permissions are refreshed according to the set permissions on the table. For information on File access permissions, see Create a Cloud file configuration on engagements and audit tasks.
   A UI message is displayed that the file has been added to the record successfully. The document is displayed in the Cloud files related list on the record form.

   The reference cloud file that is already associated to other GRC records is now linked.

### Mark a cloud file as a confidential file

Select one of the already linked files and mark it as a confidential file. Once a cloud file is marked as confidential, it cannot be linked to another record, or it cannot be referenced by any other record.

#### Before you begin
Role required: sn_audit.admin or sn_audit.manager, sn_grc_workspace.user

#### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the tasks icon ( ).
3. Select an engagement in the Engagements list.
   The list displays the engagements that are assigned to the logged-in user.
4. In the **Cloud documents** related list, select the cloud document.
5. Select **Mark as confidential**.
   When a cloud file is marked as a confidential document, it cannot be linked to other records.
   The cloud document is marked as a confidential document. It cannot be shared or referenced by any other records.

### Mark a cloud file as a non-confidential file

Select one of the confidential files and mark it as non-confidential. Once the cloud file is marked as non-confidential, it can be linked to another record, or it can be referenced by other records.

#### Before you begin
Role required: sn_audit.admin, sn_audit.manager, sn_grc_workspace.user

#### Procedure

1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the tasks icon ( ) and select a record from the list.
3. In the **Cloud files** related list, select the cloud document.
4. Select **Mark as non-confidential**.
   When a cloud file is marked as a non-confidential document, it can be linked to other records.
   The cloud file is marked as non-confidential. It can be shared or referenced by other records.

### Remove a linked cloud file from a record

Remove a linked cloud file from a record in the Audit Workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_audit.admin, sn_grc_workspace.user

### Procedure
1. Navigate to **All** > **Audit** > **Audit Workspace**.
2. Select the tasks icon (  ).
3. Select an engagement in the Engagements list.
4. In the **Cloud files** related list, select the cloud document.
5. Select **Remove linked file**.
   A confirmation pop-up is displayed with the following message: `Do you want to remove the linked file?`
6. Select **Remove linked file** in the pop-up.
   When a cloud file is linked to a record, the file access permissions are refreshed according to the set permissions on the table. For information on File access permissions, see Create a Cloud file configuration on engagements and audit tasks.
   A confirmation message is displayed that the cloud file is removed from the record.

## Manage GRC key risk and control indicators

Continuous monitoring involves activities related to identifying and creating key risk and controls indicators. Supporting information can be collected for those indicators through automatic data collection or manual tasks. Indicator results are then used to create issues for controls, update risk scores, and provide supporting information for audit activities and control testing.

Indicators collect data to monitor controls and risks, and collect audit evidence. Indicators monitor a single control or risk.

## Indicator templates

Indicator templates allow the creation of multiple indicators for similar controls or risks.

### Engagement Overview

The Engagement Overview is contained in the Audit Management application and provides an executive view into audit results, engagement breakdowns by task, and allows areas of concern to be identified quickly.

The Engagement Overview module displays audit information that is tailored to the role of the user.

## Audit Engagement Overview
Users with the Audit Administrator, Audit User, and Audit Manager roles view the Audit Engagement Overview. It contains the following reports in the base system.

**Audit Engagement Overview reports**

| Name | Visual | Description |
|---|---|---|
| Engagement Results | Column Chart | Displays an overall count of audit engagements conducted for each entity. The chart is stacked to display the overall audit results for each entity. |
| Entities by Engagement | Donut chart | Displays the total number of entities included in the scope of each audit engagement. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Audit Engagement Overview reports (continued)

| Name | Visual | Description |
|---|---|---|
| Controls by Engagement | Donut chart | Displays the total number of controls included in scope of each audit engagement. |
| Entity | Drop down list | Select one or many entities to view and compare their audit findings. |
| Select Engagement | Drop down list | Select one or many engagements to view and compare their audit findings. |
| Satisfactory Engagements | Single Score | Displays the number of engagements closed with a satisfactory result. |
| Adequate Engagements | Single Score | Displays the number of engagements closed with an adequate result. |
| Inadequate Engagements | Single Score | Displays the number of engagements closed with an inadequate result. |
| Control Test Results | Donut chart | The number of completed control tests, broken down by overall control effectiveness rating. |
| Issue Breakdown | Bar Chart | Count of issues grouped by Engagement, State, or Response |
| Audit Task Breakdown | Bar Chart | Count of audit tasks grouped by Task Type, Assigned to, Top Task and State. Stacked by Task Type, Assigned to, Top Task, and State. |
| Overdue Audit Tasks | List | List of open audit tasks that have exceeded the planned end date. |

## Create a GRC indicator

Create an Indicator to monitor the controls and risks and collect evidence of performance.

### Before you begin

Role required: compliance_admin or compliance_manager, risk_admin or risk_manager, audit_admin or audit_manager

### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Indicators** > **Indicators**.
   - **Risk** > **Indicators** > **Indicators**.
   - **Audit** > **Indicators** > **Indicators**.
2. Select **New**.
3. On the form, fill in the fields.

#### Indicator

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the indicator. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Template | Related indicator template. |
| Category | Category associated with the Control/Risk that is selected. This field cannot be edited. |
| Active | Option that determines whether the indicator is active. |
| Control/Risk | Related control or risk. |
| Applies to record | Profile related to the **Item**. |
| Owner | Owner of the indicator. |
| Owning group | Group that owns the indicator. |
| Override Template | Option to override the indicator template associated to this indicator |
| Last result passed | Option that indicates whether the controls were compliant or non-compliant. If the controls were compliant, the check box is selected. |
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| Next run time | Next collection time for indicator results. |
| Method | |
| Type | Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script.<br>◦ Manual: Used to create an Indicator task for an assignee to complete.<br>◦ Basic: Used to designate whether the indicator identifies the passed or failed controls.<br>◦ Script: Used to write a script to collect the required data. |
| Short Description | If Type is **Manual**, this field is present. Brief description of the issue. |
| Instructions | If Type is **Manual**, this field is present. Instructions for the collection of indicator results. |
| Value Mandatory | If Type is **Manual**, this field is present. |
| Passed/Failed | If Type is **Basic**, this field is present. Indicator passes or fails. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Script | If Type is **Script**, this field is present.<br>Script that obtains the required system information. |
| Supporting Data | |
| **Note:** Starting with version 10.1, the actual historical data for the supporting data records from the indicator results or indicator tasks is displayed. Earlier, only the real-time state of the records collected could be viewed. | |
| Table | Use supporting data to gather supporting evidence from other applications. |
| Supporting data fields | Supporting data fields based on the selected table. |
| Criteria | Conditions that must be met for the supporting data. |
| Sample size | Number of records to select for the supporting data. |

4. Click **Submit**.

### Create a GRC indicator template

Compliance or risk managers create indicator templates from which many indicators can be created.

#### Before you begin

Role required:

- sn_compliance.admin or sn_compliance.manager
- sn_risk.admin or sn_risk.manager
- sn_audit.admin or sn_audit.manager
- sn_grc.user

#### Procedure

1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Indicators** > **Indicator Templates**.
   - **All** > **Risk** > **Indicators** > **Indicator Templates**.
2. Click **New**.
3. On the form, fill in the fields.

##### Indicator template form

| Field | Description |
|---|---|
| Name | Name of the indicator. |
| Description | Description of the indicator. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Category | Category for which you are creating an indicator template. For example, select **Risk Indicator Template** to create a risk indicator template. |
| Active | Option that determines whether the indicator template is active. |
| Method | |
| Type | Method used to determine the type of indicator template. The choices are as follows:<br>◦ **Manual**: Manual indicators are used for data that cannot be retrieved from a ServiceNow instance because it comes from an external system, such as customer data from a third-party sales system.<br>◦ **Basic**: Basic indicators are automated indicators based on an indicator source. The indicator source specifies a table and a frequency at which the scores from this table are saved.<br>◦ **Script**: Scripted indicators use a custom script to collect the data. |
| Result if the value meets or exceeds the target value | Result configuration field. The choices are as follows:<br>◦ **Passed**<br>◦ **Failed**<br>For example, assume you enter `100` in this field. If the indicator result output is more than 100, then the indicator status will pass or fail based on the value configured in this field. |
| Target Type | Type of the target value. The choices are as follows:<br>◦ **None**: Use this option if you do not want to set up any target or threshold for the indicator.<br>◦ **Percentage**: Use this option to determine the indicator result by a percentage value.<br>◦ **Count**: Use this option to determine the indicator result by a count value or total number. |
| Target | Value to determine if the indicator will pass or fail. |
| Instructions | Additional instructions for the template. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Value mandatory | Option to decide if a value must be compulsory in the indicator task for a manual indicator.<br><br>**Note:** This option appears only if **Manual** is selected from the **Type** field. This option is automatically selected if **Count** or the **Percentage** is selected from the **Target type** field. |
| Supporting Data | |
| **Note:** Starting with version 10.1, the actual historical data for the supporting data records from the indicator results or indicator tasks is displayed. Earlier, only the real-time state of the records collected could be viewed. | |
| Collect supporting data | Option to enable collecting supporting data or evidence every time the indicator runs. |
| Table | Table used for collecting supporting data. |
| Supporting data fields | Fields of the source table to be used for collecting the supporting data. |
| Sample collection type | Type of supporting data collection, such as count or percentage. |
| Sample size | Minimum number of records that must be used for collecting supporting data.<br><br>For example, a basic indicator could query a large table, returning thousands of records with each indicator execution. You do not need to save all of them; just a sample of those records. If you enter a sample size of 100, only 100 records are saved, even though the query returned thousands. |
| Basic Criteria | |
| Criteria | Criteria to filter the data from the source table. |
| Use reference field | Option to enable the use of the **Reference field**. |
| Reference field | Connection between the supporting data table and the **Applies to record** field of the entity. |
| Additional Criteria | |
| To create indicators with targets, use the advanced filter criteria. This section appears only when you select **Basic** from the **Type** field. This section is used to provide more filter criteria. | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Additional criteria | More criteria to filter the data to calculate the target value. This section only appears when **Percentage** is selected from the **Target type** field. |
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| First run date | First collection time for indicator results. This field is automatically set based on when an indicator or an indicator template runs for the first time. The value in this field cannot be modified. |
| Next run date | Next run time to collect indicator results of all downstream indicators for this indicator template. |
| Due date duration (days) | Due date duration in days between the creation and due date of the indicator task and generation of its results.<br><br>The due date duration added to the creation date reflects as the **Due date** of the indicator task.<br><br>This field appears only when **Manual** is selected from the **Type** field.<br><br>For more information, see Performance enhancements for Indicator nightly job. |

4. When you have completed these entries, you can also view information on the following related lists:
   - Control Objectives/Risk Statements
   - Content References

   **Note:** The **Control Objectives/Risk Statements** tab enables you to reuse the same template for multiple control objectives or risk statements, or both of them.

5. Select **Submit**.

## Confidentiality flag for audit and compliance records

You can set the confidentiality flag at the record level for an issue, engagement, observation, control test, activity, interview, and walkthrough records. The users whom you determine to view and update these records are allowed users.

When the **Confidential** option is selected, a list of users who can be an engagement lead, auditors, and approvers are auto-populated as **Allowed users**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

As a system admin, you can add more audit users or GRC business users to the list or remove some of the existing users based on your access control criteria and can set them as allowed users.

Also, you can also add random users to the record, who are not audit users or GRC business users. However, an email notification is sent to all allowed users who have neither an audit user nor a GRC business user role intimating them to acquire the confidential role (sn_grc.confidential_user) from the admin if they are to access the record.

You can also select groups as **Allowed groups** who can access the record as well.

You can view all issues, remediation tasks, evidence request tasks, engagements, observations, and all audit tasks marked as confidential records from the application navigator as GRC confidential records. For more information, see Confidential records in common GRC features.

Similarly, if you are working in the Audit and Compliance workspaces, you can monitor the **Confidential records** in a separate tab in the Tasks page. For more information, see My tasks in the workspace.

To enable the Confidentiality property at the system level:

1. Navigate to **Policy and Compliance** > **Administration** > **GRC Properties**.

   **Note:** The user must have sn_grc.admin role.

2. Select **Yes** for **Enable record level confidentiality**.
3. Click **Save**.

## Manage audit issues and remediation

Issues can be created manually to document audit observations or remediations, or to accept any problems. They are automatically generated from indicator results, attestation results, or control test effectiveness.

Various types of issues are created under the following conditions:

Issue

Created when an indicator fails

Control issue

Created when a control attestation is completed indicating that the control is **Not implemented**

Control test issue

Created when a control test is closed complete with the control effectiveness set to **Ineffective**

Other issue

Created by the user manually

Remediating an issue marks an intention to fix the underlying issue causing the control failure or risk exposure. Accepting an issue marks an intention to create an exception for a known control failure or risk. Controls that are **Accepted** remain in a non-compliant state until the control is reassessed. In this way, the issue can be used to document observations during audits.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Manually create GRC issues

As a GRC user, you can manually create issues to document policy, risk, or audit observations, or to accept any GRC problems. You can also identify the source of the issue to help analyze and classify the issues.

## Before you begin

Role required: (per product)

- In Policy and Compliance Management: compliance_admin, compliance_manager, sn_compliance.user, sn_grc.business_user, sn_grc.business_user_lite
- In Risk Management: risk_admin, risk_manager, or sn_risk.user
- In Audit Management: audit_admin, audit_manager, audit_admin, or sn_audit.user

**Note:** Starting with Version 12.0.1 of the products mentioned above, the minimum role for the **Assigned to** user on the Issues form is GRC Business User [sn_grc.business_user]. The minimum role for the **Issue manager** is GRC User [sn_grc._user].

For more information on the access control limitations to issues, see GRC business user role to control access and track usage of compliance tables.

## Procedure

1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Issues** > **Create New**.
   - **Risk** > **Issues** > **Create New**.
   - **Audit** > **Issues** > **Create New**.

   **Note:** Starting with Version 12.0.1 of the products mentioned above, the minimum role for the **Assigned to** user on the Issues form is GRC Business User [sn_grc.business_user]. The minimum role for the **Issue manager** is GRC User [sn_grc._user].

2. On the form, fill in the fields.

### Issue form

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Assignment group | Group to which this issue has been assigned. Each member gets a notification when an activity happens on this issue. |
| Assigned to | Member of the group assigned to resolve the issue.<br><br>Starting with Version 12.0.1, the user must have at least the sn_grc.business_user role. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** Use the bulb icon to get suggestions on who must the issue be assigned to. The bulb icon only appears if you have the GRC: Predictive Intelligence application activated, the form is saved, the **Assigned to** field is not inactive, and the GRC Property is selected as Similarity Analysis. For more information, see .<br><br>You can configure a hierarchy of users to access the issue record. For more information, see User hierarchy access control for issue and remediation task records.<br><br>Starting with Version 12.0.1, the assigned-to user gets an email notification when the issue manager requests more information.<br><br>Starting with Version 12.0.1, when an issue transitions to the **Respond** state, an entry in the **Assigned to** field is mandatory. |
| Issue source | Source from where the issue was created. This field is auto-populated with one of the following options based on how the issue is created:<br>◦ Indicator Failure: Issue is created by a failure of the indicator<br>◦ Risk Assessment: Issue is created in a risk<br>◦ Risk Event: Issue is created in a risk event<br>◦ Control Attestation Failure: Issue is created due to a non-compliant control<br>◦ Control Test Failure: Issue is created when a control is ineffective and the control test is marked as closed and complete<br>◦ Ad-hoc: Issue is manually created |
| Issue type | Type of issue. Choices are:<br>◦ Control design effectiveness failure<br>◦ Control operative effectiveness failure<br>◦ Control does not meet requirement<br>◦ Control does not exist<br>◦ Non-compliance to a regulation<br>◦ Non-compliance to a policy<br>◦ Improvement or suggestion to an existing policy |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Recommendation for a new policy<br>◦ Process optimization or improvement<br>◦ Observation<br>◦ Data Breach<br>◦ Fraud<br>◦ Misstatement<br>◦ Training<br>◦ Documentation<br>◦ Risk issue<br>◦ Other |
| Classification | The classification of the issue as a risk, compliance, or audit, based on the issue type. |
| Issue manager group | The group responsible for managing and reviewing the issue.<br><br>Starting with Version 12.0.1, the following enhancements and requirements were introduced:<br>◦ Members of the issue manager group must have one of the following roles:<br>▪ sn_audit.manager<br>▪ sn_audit.user<br>▪ sn_compliance.manager<br>▪ sn_compliance.user<br>▪ sn_grc.manager<br>▪ sn_grc.user<br>▪ sn_risk.manager<br>▪ sn_risk.user<br>◦ When an issue transitions to the **Analyze** state, an entry in either the **Issue manager group** or **Issue manager** field is mandatory.<br>◦ When an issue is assigned to the group, the members receive an email notification. Additionally, the issue manager receives an email notification when the issue transitions to the **Review** state. |
| Issue manager | The user responsible for managing and reviewing the issue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | Starting with Version 12.0.1, the following enhancements and requirements were introduced:<br>◦ The issue manager must have at least the sn_grc.user role.<br>◦ The issue manager receives an email notification when the assigned-to user provides requested information.<br>◦ When an issue transitions to the **Analyze** state, an entry in either this field or **Issue manager** is mandatory.<br>◦ When an issue transitions to the **Respond** state, an entry in this field is mandatory. |
| State | ◦ New<br>◦ Analyze<br>◦ Respond<br>◦ Review<br>◦ Closed Complete<br>◦ Closed Incomplete |
| Substate | The substate and applicable details for the substate. |
| Priority | The sequence in which an issue must be resolved, based on its impact and urgency:<br>◦ **1 — Critical**<br>◦ **2 — High**<br>◦ **3 — Moderate**<br>◦ **4 — Low**<br>◦ **5 — Planning** |
| Issue rating | Starting with Version 12.0.1, the issue manager can assign the issue rating to the issue. Based on the issue rating, the **Due date** under the **Dates** tab is calculated as follows and displayed:<br>◦ Very high (2 days)<br>◦ High (4 days)<br>◦ Moderate (8 days)<br>◦ Low (10 days)<br>◦ Very Low (15 days)<br>You can manually override the **Due date**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** Users with the sn_grc.manager and sn_grc_advanced.issue_triage_manager role can navigate to **Policy and Compliance** > **Administration** > **Issue rating** and define additional issue ratings.p<br><br>When the issue transitions to the **Respond** state, the Issue rating field is read only. |
| Issue group rule | Group rule assigned to this issue. The Issue group rule is used to group similar issues together into a parent issue based on the conditions defined in the rule. This rule enables you to work on similar issues simultaneously and close out the parent issue after all issues are resolved. This closes out all the child issues. |
| Parent Issue | Parent issue this issue belongs to. |
| Configuration item | Item associated with this issue. If all child issues have the same configuration item, it gets copied over to the parent issue |
| Location | Location where the issue occurred. |
| Short description<br><br>Starting with Version 12.0.1, this label was changed to **Name**. | A name for the issue. |
| Description | A more comprehensive description of the issue. |
| Details | |
| Control/Risk | Control or risk associated with the issue.<br><br>When the control is associated, the corresponding entity of the control is added to the **Entity** field, and the control objective is added to the **Control Objective/Risk Statement** field. These control objective and entity are the ones that are linked to this control.<br><br>When the control is associated to the issue form, an m2m record is created in the source [sn_grc_m2m_issue_item] table. Whenever a record is added in the source table, a corresponding record, Issue to Entity is added in the destination [sn_grc_m2m_issue_to_entity] table, and another record Issue to |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | Content is added in the destination [sn_grc_m2m_issue_content] table for the associated entity and control objective of the control. |
| Entity | Related entity. |
| Policy | The policy associated with the issue. |
| Authority document | The authority document associated with the issue. |
| Control Objective/Risk Statement | The control objective or risk statement related to this issue. |
| Recommendation | Resolution actions recommended by the risk, compliance, or audit teams. |
| Action Plan | The plan for remediating the issue. |
| Dates | |
| Planned start date | Date and time that work on the issue is expected to begin. |
| Planned end date | Date and time that work on the issue is expected to end. |
| Planned duration | Estimated amount of work time for the issue. |
| Confirmed date | (Starting with Version 12.0.1) The date when the issue is confirmed. This field is read-only, and displays today's date when the issue is moved from **New** to any of the following states:<br>◦ **Analyze**<br>◦ **Review**<br>◦ **Respond**<br>**Note:** If a triage issue is converted to an actual issue, this field displays the date it was converted. |
| Due date | (Starting with Version 12.0.1) This date is auto-populated based on a GRC property. Navigate to **Policy and Compliance** > **Administration** > **GRC Properties**. If the **Auto populate due date based on issue rating** property is set to **Yes**, this field is auto-populated based on the predefined remediation time frame for the issue's risk rating. Otherwise, you can manually enter a due date.<br>When an issue transitions to the **Respond** state, an entry in this field is mandatory. |
| Actual start date | Time when work began on this issue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Actual end date | A read-only value that is determined by the **Actual duration** input field. |
| Actual duration | Amount of work time. |
| Created | The date and time the issue was created. |
| Closed | The date and time the issue was closed. |
| Engagement | |
| Engagement | The related engagement. |
| Activity | |
| Additional comments (Customer visible) | Public information about the issue. Click **Post** to add your comments to the issue. |
| Work notes | Click the **Work notes** check box to display the **Work notes** field. Information about how to resolve the issue, or steps already taken to resolve it, if applicable. Work notes are visible to users who are assigned to the issue. Click **Post** to add your work notes to the issue. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on the confidential option, see Confidentiality flag for audit and compliance records. |
| Risk Event | |
| Risk event | The related risk event. |

3. Save the issue record.
   The tabs at the bottom of the screen enable you to perform various tasks for remediating the issue. You can add policy exceptions and create remediation tasks. Additionally, you can view other issues, indicator results, and task SLAs related to the issue.

   **Note:** Starting with Version 12.0.1, the **Task SLA** tab creates and displays SLAs based on the **Due date**. Notifications are sent to the issue owner and issue manager when the issue **Due date** reaches 50%, then 75%, then when it breaches. If the **Assigned to** and **Due date** fields are not empty and the issue is not in the **New** state, an SLA is created for the issue.

   If the due date for the SLA changes, a new SLA is created. The SLA is completed when the issue transitions to **Closed Complete** or **Closed Incomplete**. Also, the SLA is cancelled if the **Due date** or **Assigned to** fields are empty, or the state is New.

   Also starting with Version 12.0.1, remediation tasks can be created with the Assigned to user and issue manager user roles, as well as any user with the GRC Business User role.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## GRC: Audit Management Analytics and Reporting Solution

Analytics and Reporting Solutions contain preconfigured dashboards. These dashboards contain actionable data visualizations that help you improve your business processes and practices.

The GRC: Audit Management Analytics and Reporting Solution is available on the ServiceNow Store.

## Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Use the Platform Analytics widgets on the dashboard to visualize data over time, analyze your business processes, and identify areas of improvement. With Platform Analytics Solutions, you can get value from Performance Analytics for your application with minimal setup. You can always create your own objects as well.

**Important:** Set up and test Platform Analytics Solutions on a non-production instance before enabling them in production.

To enable the Analytics and Reporting solution for GRC: Audit Management, perform these steps.

1. Visit the ServiceNow Store and obtain an entitlement to the Performance Analytics - GRC: Audit Management application and associated applications. See Install a ServiceNow Product on the ServiceNow Store.
2. On the instance, navigate to **System Applications** > **All Applications** > **All**.
3. Locate and install the Performance Analytics - GRC: Audit Management application.

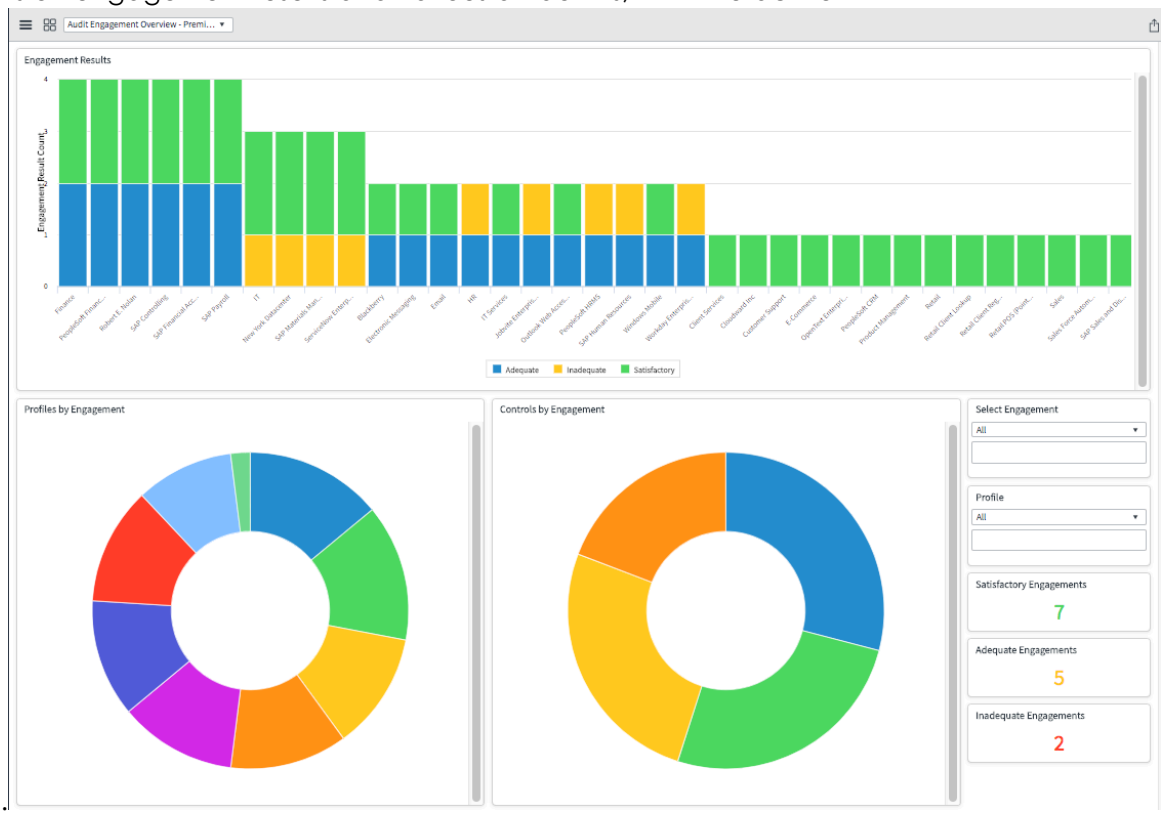
### GRC Audit Engagement Overview dashboard

The Audit Engagement Overview dashboard provides an executive view into audit results and engagement breakdowns by task, allowing areas of concern to be identified quickly.

Because this dashboard uses interactive filtering, the licensed version of Performance Analytics is required.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Audit Engagement Overview dashboard has one view, with reports on engagement results and various drilldowns, with interactive filters.




## End users

| End user and goal | Required role |
|---|---|
| Audit Manager: Needs clear visibility into the overall state and volume of vulnerabilities within the organization. | sn_audit.manager |
| Audit Administrator: Needs to pinpoint areas of concern quickly | sn_audit.admin |
| Audit Analyst: Needs to quickly prioritize which risks/tasks to focus on based upon criticality to the organization. | sn_audit.user |

## Reports

The Audit Engagement Overview dashboard contains the following reports:

| Name | Type | Description |
|---|---|---|
| Adequate Engagements | Single Score | Displays the number of engagements closed with an adequate result. |
| Audit Task Breakdown | Horizontal bar | Total number of active audit tasks broken down by type, state, and assigned to |
| Control Test Results | Donut | The number of completed control tests, broken down by overall control effectiveness rating. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Name | Type | Description |
|---|---|---|
| Controls by Engagement | Donut | Breakdown of the number of open controls by audit engagement |
| Engagement Results | Bar | Displays an overall count of audit engagements conducted for each entity. The chart is stacked to display the overall audit results for each entity. |
| Inadequate Engagements | Single Score | Displays the number of engagements closed with an inadequate result. |
| Issue Breakdown | Horizontal bar | Count of issues grouped by Engagement, State, or Response |
| Overdue Audit Tasks | List | List of open audit tasks that have exceeded the planned end date. |
| Profiles by Engagement | Donut | Select one or many entities to view and compare their audit findings. |
| Satisfactory Engagements | Single Score | Displays the number of engagements closed with a satisfactory result. |

### Audit Manager dashboard

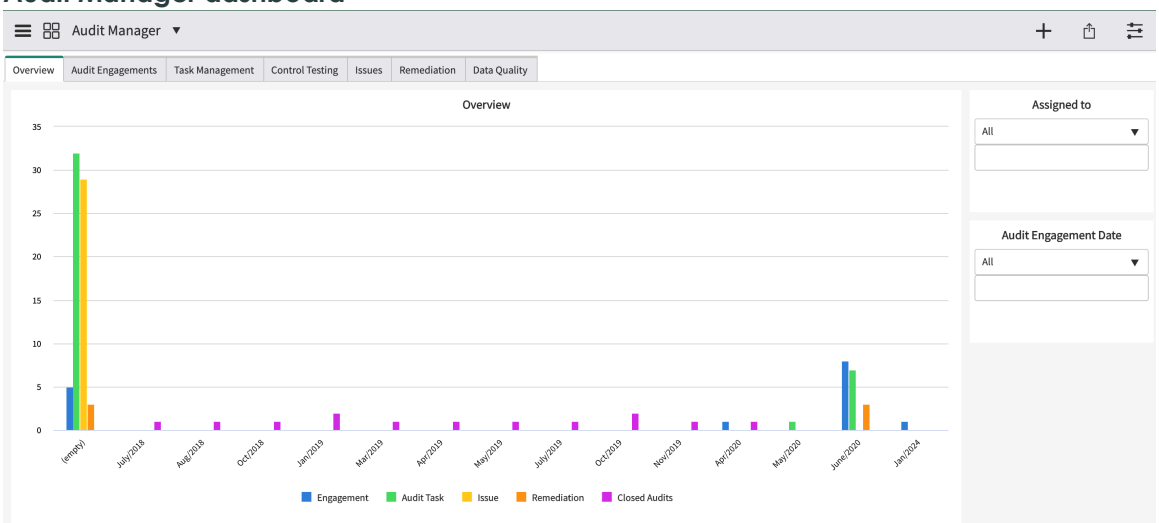
The Governance, Risk, and Compliance Audit Manager dashboard provides a current view of audit engagements and related audit activities. Users with the sn_audit.manager role can view this dashboard. This Audit Manager dashboard is part of the Advanced GRC dashboard.

**Note:** To view the Audit Manager dashboard, activate the following GRC applications:

- GRC Audit Management (com.sn_audit)
- GRC Advanced Dashboards (com.sn_grc_pa_advanced)

To view the Audit Manager dashboard, navigate to **Audit** > **Audit Manager Dashboard**. Log in with the sn_audit.manager role to view reports.

### Audit Manager dashboard




The Audit Manager dashboard provides detailed reports that capture audit activities, for example:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Overview of various open and closed engagements
- Overview of audit tasks and control test status
- Overview of audit issues and control test failures
- Active remediation tasks
- Closed audits
- Data quality of audits

This dashboard provides useful answers to the following questions:

- What are the open, past due, closed, and upcoming audits? What is the audit engagement date range? Who are the audit tasks assigned to?
- What are the key audit engagements? Are the engagement results adequate or satisfactory?
- What are the various audit tasks? What is the percentage of task completion?
- How many tests are completed over given time?
- Are the issues and remediation tasks completed on time?

Users with the sn_audit.manager role can view and adjust a report chart by grouping or stacking data. To group and stack audits and their activities, use common filters such as State, Assigned to, Result, and Name.

Various interactive filters are provided to further refine reports. For example, use the Assigned to filter to view the audits assigned to Abel Tuter.

## Overview

The **Overview** tab provides a color-coded bar chart report. It displays the latest view of the audit engagements and audit activities such as audit tasks, issues, and remediation tasks. You can further drill down in the individual reports.

Use the following interactive filters to filter data on the **Overview** tab reports:

- Assigned to
- Audit Engagement Date

## Audit Engagements

The **Audit Engagements** tab provides an overview of the audit engagements and displays the following reports.

### Audit Engagements tab

| Reports | Description |
|---|---|
| Open Audits | Number of audit engagements which are open |
| Past Due Audits | Past due audits over time |
| Upcoming Audits | Monthly count for the upcoming audit engagements |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Audit Engagements tab (continued)**

| Reports | Description |
|---|---|
| Started Audits | Monthly count for the audit engagements that have been started |
| Closed Audits | Closed audit engagements |

Use the following interactive filters to filter data on the **Audit Engagements** tab reports:

- Assigned to
- Audit Engagement Date

## Task Management

The **Task Management** tab provides an overview of the audit tasks and displays the following reports.

**Task Management tab**

| Reports | Description |
|---|---|
| Active Tasks | Number of active tasks |
| Past Due Tasks | Past due tasks |
| Tasks Due This Week | Tasks that are due in a given week |
| Upcoming Audit Tasks | Upcoming audit tasks |
| Tasks Completed On-Time | Number of tasks completed by the users on time |
| Tasks Completed After Planned End date | Tasks that are completed after the planned end date |
| Tasks Completed | Number of tasks completed over time |

Use the following interactive filters to filter data on the **Task Management** tab reports:

- Assigned to
- Audit Engagement Date
- Task Type

  The example task types are interviews, walkthroughs, activities, and control tests.

## Control Testing

The **Control Testing** tab provides detailed information on control tests. On further drill down, you can view detailed information about the control tests. This tab displays the following reports.

**Control Testing tab**

| Reports | Description |
|---|---|
| Active Tests | Number of active tests |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Control Testing tab (continued)**

| Reports | Description |
|---|---|
| Past Due Tests | Number of past due tests |
| Tests Due This Week | Tests that are due in a given week |
| Upcoming Tests | Upcoming control tests |
| Tests Completed On-Time | Number of tests completed on time |
| Tests Completed After Planned End date | Tests that are completed after the planned end date |
| Open Tests by Week | Tests that are open in a given week |
| Tests Completed by Month | Number of tests completed in a month |

Use the following interactive filters to filter data on the **Control Testing** tab reports:

- Assigned to
- Audit Engagement Date
- Operation Effectiveness
- Design Effectiveness

## Issues

The **Issues** tab provides an overview of all the issues that are created under audit and the issues that are generated due to control test failures. This tab displays the following reports.

**Issues tab**

| Reports | Description |
|---|---|
| Active Issues | Number of active issues assigned to different users |
| Past Due Issues | Past due issues assigned to different users |
| Issues Awaiting response | Issues that are open and awaiting response |
| Issues Due This Week | Issues that are due in a given week |
| Upcoming Issues | Number of upcoming issues |
| Issues Completed Before Planned End date | Issues that are completed before the planned end date |
| Issues Completed After Planned End date | Issues that are completed after the planned end date |
| Issues Completed On-Time | Number of issues completed on time by the users |
| Issues Completed by Month | Number of issues completed in a month |

Use the following interactive filters to filter data on the **Issues** tab reports:

- Assigned to
- Audit Engagement Date

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Issue Entity
- Issue State
- Issue Priority
- Issue Response

## Remediation

The **Remediation** tab provides an overview of the remediation tasks created for the audit issues and displays the following reports.

**Remediation tab**

| Reports | Description |
|---|---|
| Active Remediation Tasks | Number of active remediation tasks |
| Past Due Planned Remediation | Number of past due remediation tasks |
| Remediation Tasks Due This Week | Remediation tasks that are due in a given week |
| Upcoming Remediation Tasks | Remediation tasks that are forthcoming |
| Remediation Tasks Completed Before Planned End date | Remediation tasks that are completed before the planned end date |
| Remediation Tasks Completed After Planned End date | Remediation tasks that are completed after the planned end date |
| Remediation Tasks Completed On-Time | Number of remediation tasks completed on time by the users |
| Remediation Tasks Issues Completed by Month | Number of remediation tasks completed in a month |

Use the following interactive filters to filter data on the **Remediation** tab reports:

- Assigned to
- Audit Engagement Date
- Remediation Task Priority

## Data Quality

The **Data Quality** tab provides the reports to validate whether the data for audits, audit issues, remediation tasks, and control tests is captured in a correct manner. This tab displays the following reports.

**Data Quality tab**

| Reports | Description |
|---|---|
| Active Audits No Assignee | List of unassigned active audits |
| Audits Without Tasks | List of audits without tasks |
| Active Audits No Entity | List of active audits with no entities |
| Audit Task No Assignee | List of unassigned audit tasks |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Data Quality tab (continued)**

| Reports | Description |
|---|---|
| Operation Test No Result | List of operation tests with no results |
| Active Audits No Description | List of active audits with no description |
| Design Test No Result | List of design tests with no results |
| Issues No Description | List of issues with no description |
| Control Test No Assignee | List of unassigned control tests |
| Issues No Assignment Group | List of issues with no assignment group |
| Issues No Remediation Tasks | List of issues with no remediation tasks |
| Control Test No Test Plan | List of control tests with no test plans |
| Issues No assignee | List of unassigned issues |
| Issues No Recommendation | List of issues with no recommendation |
| Issues No Explanation | List of issues with no explanation |
| Remediation Task No Assignee | List of unassigned remediation tasks |
| Issues No item | List of issues with no items |
| Remediation Task No Issues | List of remediation tasks with no issues |

Use the Assigned to filter in the report to filter data on the **Data Quality** tab reports.

Related topics

Advanced Governance, Risk, and Compliance Application Risk dashboard

## Evidence request

Evidence request is used by audit and compliance teams for requesting supporting documents during an audit. Auditors and compliance teams require these documents from the first line of defense.

Evidence is all the information used by an auditor in determining the audit opinion. Evidence includes the information contained in the accounting records underlying the financial statements and other information. Evidence is cumulative in nature. It includes evidence obtained from audit procedures performed during the audit. Evidence may also include audit evidence obtained from other sources such as, previous audits.

An evidence request is frequently introduced during the audit preparation or the planning phase after the audit announcement. The documents requested are used by the audit team to understand the in-scope controls and processes, and to begin fieldwork testing. As an audit progresses through various stages, the audit team frequently adds new requests to the list. The compliance teams use the collected evidence for control testing. Starting with the latest release, unplanned evidence request is supported by Audit Management and Policy and Compliance Management. The following are the benefits of the evidence request feature:

- Helps the second line and third line of defense to create and send all their evidence requests quickly.
- Helps in the management of requests and evidence.
- Eliminates multiple emails by providing a tool for communication.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Compliance teams can request evidence from control owners, business stakeholders, and process owners.
- Audit teams can request evidence from control owners, business stakeholders, process owners, and compliance teams.
- Enables providing the due date for the evidence to be submitted.
- Provides the ability to send email reminders to the assignee.
- The assignee can provide evidence directly from the Service Portal.
- Simplified manager approval of evidence requests can be based on various criteria, such as confidentiality and criticality.
- The assignee can store evidence in a common evidence folder, such as Box or SharePoint.
- Improved communication channels between requesters and assignees streamline the approval process.
- Improved confidentiality constraints prevent unauthorized persons from viewing request information.

Evidence can be requested from an engagement and all audit tables. To understand how to request evidence, refer to Request evidence for audit.

## Evidence request workflow and users

Evidence request helps customers to electronically request the information that they need from the first and second line of defense. The individuals being audited can then immediately upload their documents to the system, significantly reducing manual processing time.

The evidence request workflow is as follows:

1. An audit user with the sn_audit.user role requests evidence and assigns the request to another user. This requester can either request the evidence for themselves or raise a request on behalf of another audit user or GRC user. If the requester determines that an evidence task has been created erroneously, then the requester can cancel that particular evidence task. The ability to cancel the evidence request is available when the request is in **Draft** state. A requester can cancel the evidence request tasks any time until the tasks reach the **Review** state.
2. After you create an evidence request, you must create evidence collection records and then the requester must request evidence. Evidence Collection records contain the evidence collection instructions, assigned to, and assignment group. On clicking **Request Evidence**, evidence request tasks are generated and they are assigned to a group or user.
3. The assignee then receives an email with the link to provide the requested evidence.

   **Note:** If the requester changes the assignee after requesting evidence, then the original assignee can no longer view the request. Only the person who is assigned the request can view the request. This feature ensures confidentiality.

4. The assignee can either attach the requested evidence or provide a URL or location that contains the required evidence.
5. The assignee can also add an approver for verifying and approving the evidence. Adding approvers is necessary if the evidence is sensitive and confidential in nature.
6. The approver can then review the evidence and either approve it, request revision, or request further details about the evidence.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. If the approver approves the evidence, the requester receives the evidence and can process it further.
8. The requester can then review the evidence and do one of the following:
   - accept the evidence.
   - request for its review.
   - request further details about the evidence.
   - cancel the evidence request if it is not required anymore.
   - delete the request.
9. If the requester accepts all the evidence tasks, the request is closed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The evidence request workflow is shown in the following

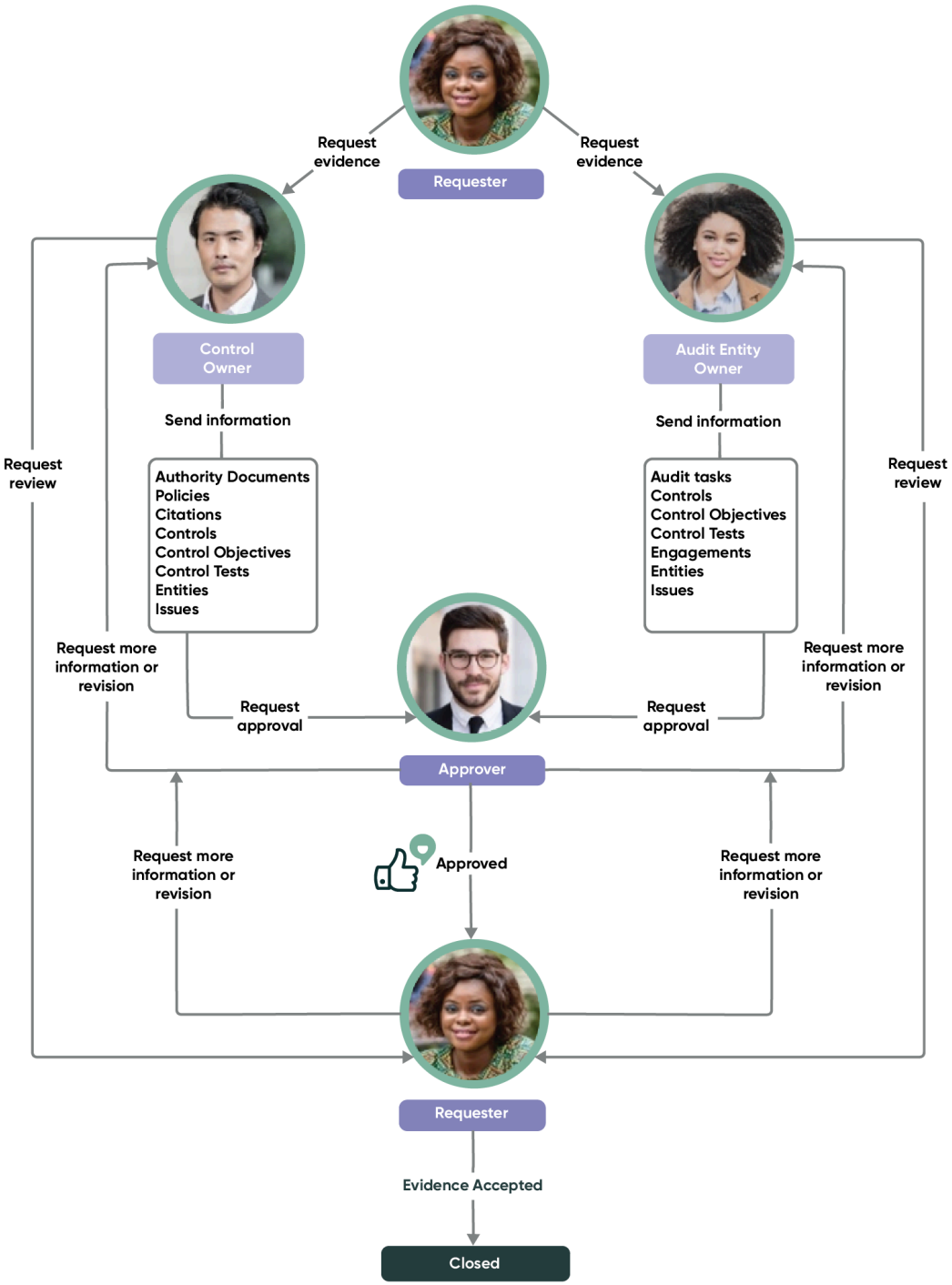



figure:

The following table describes the roles and their responsibilities during the evidence request workflow:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Evidence request users, responsibilities, and requirements**

| User | Responsibilities | Requirements |
|---|---|---|
| Internal auditor | • Perform audit testing.<br>• Request audit testing.<br>• Review all audit findings and the evidence collected. | • Visibility into compliance and risk activity.<br>• A job queue (pending, current, upcoming) to plan their team efforts.<br>• Track and monitor audit findings.<br>• Track and monitor audit activities. |
| Compliance manager, Audit manager | • Can request evidence.<br>• Request compliance test evidence.<br>• Review all findings and evidence collected. | • Visibility into compliance activities.<br>• A job queue (pending, current, upcoming) to plan their team efforts.<br>• Track and monitor compliance findings. |
| Compliance user, Control owner | • Ensure that the controls are implemented.<br>• Attest to the controls.<br>• Test the controls.<br>• Provide audit evidence requested by the auditor. | • A job queue to direct their day-to-day activities.<br>• Track the time spent and performance of activities and tasks they own.<br>• Ensures the task they own and additional request from the auditor is fulfilled. |

### Request evidence for audit

Request evidence at any stage during an audit. The details about the items for which evidence is requested are also provided to the person responsible for providing the evidence.

## Before you begin

Role required: sn_audit.user

## About this task

An evidence can be requested in the following three ways:

- By creating an evidence record from the **My Evidence** module.
- From the Entity, Control, Audit Task, Control Test Issue, and Other Issues related lists in an engagement record. To request evidence from these sources, navigate to **Audit** > **Engagements** > **My Engagements**. Open the engagement record, and select the related list from which you want to request evidence. From the **Action on selected rows** list, select **Request Evidence**. Here, you can either create a new evidence request or add

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

more requests to an existing evidence request. The Evidence request is created but not evidence request tasks.

- From the following tables: Entity, Control, Control Objective, Control Test, Engagement, Issue. However, when the users request evidence from these tables, the evidence request is created not the actual evidence request task. The users must go to the evidence request record that is generated and then add evidence request tasks.

In this procedure, the method to request evidence from the **My Evidence** module is described.

### Procedure

1. Navigate to **Audit** > **My Evidence Request**.
2. Click **New**.
3. On the form, fill in the fields.

**Evidence Request form**

| Field | Description |
|---|---|
| Number | Unique number of the evidence request. |
| Requester | User requesting evidence. This field is automatically populated. |
| Requested on behalf of | User for whom evidence is being requested. |
| Assignment group | Group assigned to provide evidence. |
| Assigned to | User responsible for providing the evidence. |
| State | State of the request. The default state is **Draft**. |
| Type | The default type is **Audit**. |
| Request reason | Reason for requesting evidence. |
| Watch list | Users interested in viewing the evidence collected. If a person is added on the watch list, they can navigate to **Audit** > **Evidence Request** > **Watched Evidence Requests** to view the requests. |
| Short description | Brief description of the evidence request. |
| Description | Detailed description of the evidence request. |
| Schedule | |
| Due date | Expected date of evidence submission. |
| Opened | Date the request is opened. This date is automatically updated. |
| Closed | Date the request is closed. This date is automatically updated. |
| Activity | |
| Work notes | Type any notes that might be required. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Activities | Activity log for the request. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |

4. Save the form.
   The Evidence Collection Details related list appears. This related list is used to list the items for which evidence is requested.
5. Click **New**.
6. On the form, fill in the fields.

**Evidence Collection Detail form**

| Field | Description |
|---|---|
| Evidence request | Unique number of the evidence request task. |
| Evidence for | Record for which evidence is requested. |
| Assignment group | Group assigned to provide evidence. The users of this group must have the sn_grc.business_user roles. |
| Assigned to | User responsible for providing evidence. |
| Evidence collection instructions | Instructions for providing evidence. For example, list of supporting documents, files, and so on. |

7. Click **OK**.
8. Click **Submit**.
9. Click **Request Evidence**.
   When an evidence request is already in the Work in Progress state, and a new evidence collection detail is added, then evidence request task is sent to the assignee immediately. The Evidence related list appears with the list of evidences and the person who is assigned the request receives an email notification to provide the requested evidence. Also, the state of the request changes to **Work in Progress**.

### Provide requested evidence

Provide evidence when you are requested. When evidence is requested, the person who must provide the evidence receives an email. The process to provide the evidence begins.

**Before you begin**
Role required: sn_grc.business_user

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

When the assignee receives the email to provide the requested evidence, the assignee can either provide the requested evidence or reassign the request to another user. The assignee can also add approvers before sending the requested evidence to ensure additional security of the evidence. If the assignee reassigns the request to some other user, the original assignee can no longer view the request. If the evidence provided does not need an approver, then the assignee can directly request a review of the evidence, and the requester gets a notification to review the evidence.

### Procedure

1. Navigate to **All** > **Audit** > **Evidence Request** > **My Evidence Request Tasks**.
2. Open the record for which you want to provide evidence.
3. Click **Accept Work**.
4. On the form, fill in the fields.

| Field | Description |
|---|---|
| Number | Number of the evidence request. This value is generated by default. |
| Requester | User requesting evidence. This value is generated by default. |
| Requested on behalf of | User for whom evidence is being requested. This value is generated by default. |
| Assignment group | Group assigned to provide evidence. The users of this group must have the sn_grc.business_user roles. |
| Assigned to | User responsible for providing the evidence. This value is generated by default. |
| State | State of the request. |
| Substate | None. This value is generated by default. |
| Request reason | Reason for requesting evidence. |
| Approvers | Users to approve evidence before it is returned to the requester for review. Usually, an approver is the manager of the person providing the evidence. |
| Watch list | Users interested in viewing the evidence collected. |
| Short description | Brief description of the evidence request. This description is generated by default and is fetched from the record that was created to request evidence. |
| Description | Detailed description of the evidence request. This value is generated by default and is fetched from the record that was created to request evidence. |
| Request Details | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Evidence request | Unique ID of the evidence request associated with the task. This value is generated by default and is fetched from the record that was created to request evidence. |
| Evidence for | Record for which the evidence is requested. |
| Evidence for description | Description of the record for which the evidence is being requested. This value is generated by default and is fetched from the record that was created to request evidence. |
| Evidence URL | URL of the evidence if the user prefers to share the evidence as a link instead of an attachment. For example, this can be a link to a shared folder. |

5. To request approval for the attached evidence, click **Request Approval**.
6. If no approvers are required, click **Request Review**.

### Approve evidence before evidence review

Approve the evidence being provided before the requester views the evidence. When evidence is provided in response to an evidence request, the evidence may need an approval before the evidence is sent back to the requester. This ability ensures security and confidentiality of the evidence.

#### Before you begin

Role required: sn_grc.business_user

#### About this task

After receiving a request to approve evidence, an approver can do one of the following:

- Approve the request if there are no issues or concerns.
- Request revision of the evidence attached in case it is not correct or needs rectification.
- Request information if the approver wants more details about the attached evidence.

#### Procedure

1. Navigate to **All** > **Audit** > **Evidence Request** > **My Approvals**.
2. Open the record for which you want to approve evidence.
3. Review the attached evidence on the form and click one of the following options:

| Option | Description |
|---|---|
| **Approve** | Approve the attached evidence. The requester gets the evidence provided. |
| **Request Revision** | Request that the attached evidence be reviewed. Enter comments when you request revision. The assignee gets |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
|---|---|
| | a notification to review the attached evidence. |
| **Request Information** | Seek more information and details about the attached evidence. The assignee gets a notification to provide more information about the attached evidence. |

### Accept, reject, or cancel evidence request

Accept, reject or cancel an evidence request when you receive the evidence you requested. After requesting an evidence request, when the requester receives the evidence, the requester can accept, reject, or cancel the evidence request.

#### Before you begin

Role required: sn_audit.user and sn_compliance.manager

#### Procedure

1. Navigate to **All** > **Audit** > **Evidence Request** > **My Pending Reviews**.
2. On the Evidence form, review the attached evidence, and click one of the following options:

| Option | Description |
|---|---|
| **Accept Evidence** | Accept the evidence that is provided. |
| **Request Revision** | Request for the evidence to be reviewed, if it is not appropriate, or modified. |
| **Cancel** | Cancel the evidence request task. |
| **Delete** | Delete the evidence request task. |

## Audit plan overview

An audit plan enables you to plan all your audit engagements in a systematic and logical manner.

An audit engagement is like a project which involves multiple tasks and it is difficult to manage all audit activities without planning well. Having a well-defined plan with all the audits, their projects, and costs helps audit managers to perform their tasks efficiently.

### Audit plan uses and benefits

An audit team conducts multiple audits in an organization. Creating an audit plan enables the audit teams to plan their audits and engagements better. By creating an audit plan, the auditor directors or audit leads with the role sn_audit.manager can:

- Plan engagements effectively and ensure that the goals set in the annual internal audit plan are accomplished.
- Help the auditor obtain appropriate evidence for the circumstances.
- Keep audit costs at a reasonable level.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Ensure that potential problems are promptly identified
- Get the scope of the audit program determined by an auditor to perform the audit tasks in a well-defined manner.

## Audit planning workflow

- Defining the purpose of the audit
- Risk assessment
- Audit scoping
- High-level audit schedule and detailed audit timeline with milestones
- Resource planning by necessary skills and building audit team
- Cost planning

When you create an audit plan with advanced planning capabilities and add engagements to the plan, and move the engagement to either **Validate** or **Fieldwork** state, an associated engagement project is automatically generated.

**Note:** A project is only created if the PPM Standard plugin is installed and the user has the it_project_manager role. If the user does not have the it_project_manager role and has only the sn_audit.manager role, even when advanced planning capabilities are enabled on the plan, the engagements do not have corresponding projects when they move into **Validate** or **Fieldwork** states.

After you add engagements to an audit plan, you also have the flexibility to change the parent plan of the engagements. It is important to note the following points:

- Engagements can be either added or removed from a plan only when the plan is in **Draft**, **Awaiting Approval**, and **Approved** states.
- The parent plan can only be changed on an engagement when the engagement is in **Scope**, **Validate** and, **Fieldwork** states.

## Create an audit plan

Create an audit plan to manage different types of audits in a periodic manner and group engagements in a logical manner.

### Before you begin

Role required: sn_audit.manager and it_project_manager to create projects.

Activate the Advanced Audit plugin (com.sn_audit_advanced).

### About this task

When an audit plan is created and engagements are added to the plan, the plan is sent to the approver for approval.

### Procedure

1. Navigate to **All** > **Audit** > **Plans** > **Create New**.
2. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Plan form

| Field | Description |
|---|---|
| Number | Unique number of the plan. |
| Name | Name of the plan. For example, Annual Audit Plan for Payroll. |
| Timeframe | Duration of the plan. The choices are:<br>◦ Annual<br>◦ Semi-annual<br>◦ Quarter<br>◦ Other |
| Start date | Date the plan begins. |
| End date | Date the plan ends. This field is automatically populated based on the choice made in the **Timeframe** field. If the **Timeframe** field has **Other**, then enter an end date manually. |
| Owning group | Group responsible for owning the plan. |
| Owner | Plan owner. |
| State | State of the plan. The default state is **Draft**. |
| Substate | Substate of the plan. The value in this field changes based on the workflow. |
| Type | Type of the plan. The choices are:<br>◦ None<br>◦ Internal Audit Plan<br>◦ External Audit Plan<br>◦ SOX Audit<br>◦ Compliance Audit Plan<br>◦ Vendor Audit Plan<br>◦ Customer Audit Plan |
| Plan with | Planning capability to use for the engagements. The choices are:<br>◦ Basic planning capabilities:<br>◦ Advanced Planning capabilities: If you select this option, engagement projects are automatically created. |
| Approvers | Person who approves the plan. |
| Description | Brief description of the plan. |
| Objectives | Objectives of the plan. |
| Expenses and Resources | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Budgeted expenses | Budget allocated for the engagements under the plan. |
| Planned expenses | Rolled up planned expenses from the engagements. |
| Actual expenses | Rolled up actual expenses from the engagements. |
| Expense comments | Notes about the expense details. |
| Budgeted resources | Number of hours allocated for the engagements under the plan. |
| Planned resources | Rolled up planned resources from the engagements. |
| Actual resources | Rolled up actual resources from the engagements. |
| Resource comments | Notes about the resource details. |

3. Save the form.
   The Engagements related list appears.
4. In the Engagements related list, add engagements by either clicking **New** or **Edit**.
5. Click **Request Approval**.
   The state changes from **Draft** to **Awaiting approval**.

## Approve a plan

Approve a plan if you're assigned as an approver after plan creation. You can also request that the plan be reviewed or request more information about the plan from the plan creator.

### Before you begin

Role required: sn_audit.manager

### Procedure

1. Navigate to **All** > **Audit** > **My Plan Approvals**.
2. Select and open the plan you want to approve.
3. Review the plan and click one of the following options:

| Option | Description |
|---|---|
| **Approve** | Approve the plan that is created. |
| **Request Revision** | Request for the plan to be reviewed or modified, if it is not appropriate. |
| **Request Information** | Request more information about the plan. |
| **Cancel** | Cancel the plan. |

## Create an engagement with advanced planning

Use the advanced planning capabilities to create an engagement that automatically creates an engagement project. After an engagement project is created, you can add

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

resource plans and cost plans to the engagement. The values of these plans roll up to the engagement and to the audit plan.

**Before you begin**
To use the advanced planning feature, you must activate the following store applications and plugins:

- GRC Advanced Audit plugin (com.sn_audit_advanced)
- GRC Profiles
- GRC Policy and Compliance Management
- GRC Risk Management
- GRC Advanced Core
- GRC Advanced Risk
- GRC Audit Management
- Project Portfolio Management Standard

You can choose to create audit plans for the engagement.

Role required: sn_audit.manager

**Procedure**

1. Navigate to **All** > **Audit** > **Engagements** > **Create New**.
2. On the form, fill in the fields.

**Engagement form**

| Field | Description |
|---|---|
| Number | Unique identification number of the engagement. |
| Name | Name of the engagement. |
| Type | Type of engagement. The choices are as follows:<br>◦ None<br>◦ Internal Audit<br>◦ External Audit<br>◦ SOX Audit<br>◦ IT Audit<br>◦ Financial Audit<br>◦ Compliance Audit<br>◦ Certification Audit<br>◦ Regulatory Audit<br>◦ Operational Audit<br>◦ Continuous Audit<br>◦ Vendor Audit<br>◦ Customer Audit |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Store Audit<br>◦ Quality Audit<br>◦ Project Audit<br>**Note:** For more information on the types of audits, see Audit types. |
| Assigned to | User assigned to the engagement. |
| State | State of the engagement. The choices are as follows:<br>◦ Scope<br>◦ Validate<br>◦ Fieldwork<br>◦ Awaiting Approval<br>◦ Follow Up<br>◦ Closed Complete<br>◦ Closed Incomplete<br>**Note:** For more information on each of these states, see Manage engagements. |
| Percent complete | Percentage of the engagement that is complete. |
| Auditors | Auditors assigned to the engagement. |
| Approvers | Approvers assigned to the engagement. |
| Description | General description of the engagement. |
| Objectives | Stated objectives of the engagement. |
| Schedule | |
| Engagement planned start | Estimated start date of the engagement. |
| Engagement starts | Choice to automatically determine the start date of the engagement. The choices are as follows:<br>◦ Scope<br>◦ Validate<br>◦ Fieldwork |
| Engagement actual start | Actual date when the engagement begins. |
| Engagement planned end | Estimated end date of the engagement. |
| Engagement ends | Choice to automatically determine the end date of the engagement. The choices are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Follow Up<br>◦ Closed<br>**Note:** For more information on the Follow Up and Closed states, see Manage engagements. |
| Engagement actual end | Actual date the engagement ends. |
| Fieldwork planned start | Estimated start date of the fieldwork. |
| Fieldwork planned end | Planned end date that was originally set in the engagement.<br>**Note:** This field is automatically set to one day after the planned start date for fieldwork. |
| Fieldwork planned duration | Number of days and hours planned for fieldwork. The duration and planned start date of fieldwork are used to calculate the planned end date. If audit tasks are defined, this field is automatically set to the longest planned duration from the audit tasks. |
| Fieldwork actual start | Actual start date of the fieldwork. If audit tasks are defined, this field is automatically set to the earliest actual start date from the audit tasks. |
| Fieldwork actual end | Actual end date of the fieldwork. If audit tasks are defined, this field is automatically set to the latest actual end date from the audit tasks. |
| Fieldwork actual duration | Duration of fieldwork start date and end date. |
| Results | |
| Result | Results of the engagement. The choices are as follows:<br>◦ Satisfactory<br>◦ Adequate<br>◦ Inadequate |
| Opinion | Justification for the selected result. |
| Report | |
| Knowledge base | Knowledge base to use to select the report template. |
| Report template | Template that is used to generate the knowledge base article which reports the engagement results. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| KB article | Recently generated knowledge base article which contains the engagement results. |
| Activity | |
| Additional comments | Comments that are viewable by customers. |
| Work notes | Comments that are viewable by the administrator and by the audit manager. |
| Plan Details | |
| Parent plan | Plan to associate the engagement with. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |
| Expenses and Resources | |
| Budgeted expenses | Budgeted expenses for the engagement. |
| Planned expenses | Estimated expenses for the engagement. If the cost plan is defined, this field automatically displays the estimated expenses. |
| Remaining budgeted expenses | Difference between **Budgeted expenses** and **Planned expenses**. This field is automatically set. |
| Actual expenses | Actual expenses incurred. If timecards are defined, this field is automatically set. |
| Budgeted resources | Budgeted resources for the engagement, in hours. |
| Planned resources | Estimated resources for the engagement, in hours. If resource plans are defined, this field is automatically set. |
| Actual resources | Actual resources for the engagement, in hours. If timecards are defined, this field is automatically set. |
| Project Details | |
| Project | Automatically created engagement project. This field is populated when you click **Validate and Plan**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** This field also gets populated when you click **Enable Advanced Planning** on the engagement, in the Validate or Fieldwork state. This field also gets populated if any of the following are true:<br>◦ The field is already linked to a plan with advanced planning capabilities.<br>◦ The user has the required roles.<br>◦ The engagement is in the correct state. |
| Time card approver | Person assigned to the engagement. You can also change the approver in this field.<br>**Note:** If more than one user is selected, then everyone on the list must approve the time cards. |

3. Click **Validate and Plan**.

   **Note:** The **Validate and Plan** button only appears if the Advanced Audit plugin is activated.

   The project details are populated.
4. Click **Enable Advanced Planning**.

**Result**
An engagement project is created in the background for the engagement. The Resource Plan and Cost Plan related lists also appear.

**What to do next**
Create a resource plan and Create a cost plan.

## Add auditors for an engagement from resource plans

Assign audit tasks to auditors in an engagement from the resource plans. Resource plans track the cost associated to auditors. Considering this cost is important while planning the engagement.

**Before you begin**
If you have an engagement record with a resource plan created, the resource plan must be in Allocated state. The users in the Resource Allocations section of the resource plan contain resources that can be added as auditors. The auditors you add must have sn_audit.user or external auditor role, and pps_resource role. The Resource Plans related list with its associated workflow is only available when the GRC Advanced Audit and the Project Portfolio Management plugins are activated.

Role required: sn_audit.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Audit** > **Engagements**.
2. Open the engagement record to which you want to add auditors.
3. Click the Resource Plan related list.
4. Click the **Add Auditors** button.
   The resources who have the required roles are automatically added to the auditors field, if they are not already present.

## Create an auditable unit

Create auditable units with entities such as business units, departments, vendors, products, business processes, business applications, locations, authority documents, and policies to perform risk assessments on the auditable units.

### Before you begin

Role required: sn_audit.user or sn_audit.manager

Activate the GRC Advanced Audit plugin (com.sn_audit_advanced).

### About this task

You can create an auditable unit and decide the type of risk assessment you want to perform on the auditable unit. After the risk assessment is done, based on the risk ratings, the audit managers can decide if they want to audit the entities. You can scope an auditable unit as an entity on an engagement.

### Procedure

1. Navigate to **All** > **Audit Universe** > **All Auditable Units**.
2. Click **New**.
3. On the form, fill in the fields.

**Auditable Unit form**

| Field | Description |
|---|---|
| Number | Unique number of the auditable unit. |
| Name | Name of the auditable unit. For example, Accounts Payable - Finance. |
| Owning group | Group that owns the auditable unit. |
| Owner | Owner of the auditable unit. |
| State | State of auditable unit. The default state is **Draft**. |
| Priority | Priority of the auditable unit. |
| Description | Brief description of the auditable units. |
| Risk Assessment | |
| Method | Type of risk assessment to obtain the risk rating of the auditable unit. The choices are: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ Basic Risk Assessment. This option allows you to manually enter a value for the risk rating.<br>◦ Detailed Risk Assessment. This option appears when the Advanced Audit plugin is activated. When you select this option, the Risk Assessments related list appears. |
| Risk rating | Risk rating of the auditable unit obtained from a basic risk assessment. This field appears if the **Method** field has **Basic Risk Assessment**. |
| Inherent risk rating | Inherent risk score. The value in this field is derived from advanced risk assessment. This field appears if the **Method** field has **Detailed Risk Assessment**. |
| Control effectiveness | Control effectiveness score. The value in this field is derived from advanced risk assessment. This field appears if the **Method** field has **Detailed Risk Assessment**. |
| Residual risk rating | Residual risk score. The value in this field is derived from advanced risk assessment. This field appears if the **Method** field has **Detailed Risk Assessment**. |

4. If you have selected **Basic Risk Assessment** in the **Method** field, click **Submit**.
5. If you have selected **Detailed Risk Assessment** in the **Method** field, click **Assess Risk**.
   a. In the **Assessor** field, select an assessor for the risk assessment.
   b. In the **Approver** field, select an approver for the assessment.
   c. Click **Submit**.
   A risk assessment instance link is created at the top left and the assessor gets a notification to perform the risk assessment. After the detailed risk assessment is performed, the Risk Assessments related list shows the assessment.
6. Click the following available related lists, and add entities to them as required.
   ◦ Business Units
   ◦ Departments
   ◦ Vendors
   ◦ Products
   ◦ Business Processes
   ◦ Business Applications
   ◦ Locations
   ◦ Authority Documents
   ◦ Policies

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Audit types

There are many types of audits and each of the audit types has a specific use in an audit engagement.

| Audit Type | Description |
|---|---|
| Internal Audit | An internal audit checks a company's internal controls, corporate governance, and accounting processes. |
| External Audit | An external audit is an independent examination of the financial statements prepared by the organisation. |
| SOX Audit | A Sarbanes Oxley (SOX) compliance audit is a measure of how well your company manages its internal controls. While SOX doesn't specifically mention information security, for practical purposes, an internal control is understood to be any type of protocol dealing with the infrastructure that handles your financial data. |
| IT Audit | An IT audit is the examination and evaluation of an organization's information technology infrastructure, policies and operations. |
| Financial Audit | A financial audit is an independent, objective evaluation of an organization's financial reports and financial reporting processes. The primary purpose for financial audits is to give regulators, investors, directors, and managers reasonable assurance that financial statements are accurate and complete. |
| Compliance Audit | A compliance audit is an independent evaluation to ensure that an organization is following external laws, rules, and regulations or internal guidelines, such as corporate bylaws, controls, and policies and procedures. |
| Certification Audit | A certification audit is an audit your registrar conducts to verify conformance against the ISO 9001 standard before they issue your official ISO 9001 certificate. |
| Regulatory Audit | The aim of a regulatory audit is to verify that a project is compliant with regulations and standards. |
| Operational Audit | An operational audit is an examination of the manner in which an organization conducts business, with the objective of pointing out improvements that will increase its efficiency and effectiveness. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Audit Type | Description |
| --- | --- |
| Continuous Audit | A continuous audit is an internal process that examines accounting practices, risk controls, compliance, information technology systems, and business procedures on an ongoing basis. Continuous audits are usually technology-driven and designed to automate error checking and data verification in real-time. |
| Vendor Audit | A vendor audit is performed for a company that aims to attain an objective assessment of its contractors' or vendors' compliance to the terms, conditions and intent of the contracts or agreements between two entities. |
| Customer Audit | A customer audit is a detailed review of how your company is perceived by its customers, a review of each customer's needs, and an evaluation of the role your company is playing in each of your customer's businesses. |
| Store Audit | A store audit assesses the health of your retail location using hard data. Retailers, staff, or a third party combs through your store or pop-up shop to collect information on what's working and what's selling or what isn't. |
| Quality Audit | A Quality audit is the process of systematic examination of a quality system carried out by an internal or external quality auditor or an audit team. |
| Project Audit | A project audit is a formal review of a project, often intended to assess the extent to which project management standards are being upheld. Audits are generally carried out by a specially designated audit department, the Project Management Office, an approved management committee or an external auditor. |

## Manage milestones

Milestones can be used to track the progress of an engagement.

After you create milestones for an engagement, you can also add audit tasks to the milestone and track those tasks as milestones. You can assign the milestone to a user who is responsible for the milestone. When a person is assigned to a milestone, they receive a notification informing them of the assignment. The user who is assigned the milestone must have the sn_audit.user role. When an engagement moves to the **Follow Up** state, if there are no open audit tasks, open milestones, and open observations, then the engagement moves to the **Closed** state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After you create a milestone from an engagement, you can manage your milestones by navigating to **Audit** > **Milestones** > **My Milestones**.

## Create an engagement milestone

Create milestones for an engagement to track the progress of an engagement. You can also add audit tasks to a milestone.

### Before you begin

Activate the Advanced Audit plugin.

Role required: sn_audit.manager

### Procedure

1. Navigate to **All** > **Audit** > **Engagements**.
2. Open the engagement for which you want to create a milestone.
3. Click the Milestones related list.
4. Click **New**.
5. On the form, fill in the fields.

#### Milestone form

| Field | Description |
|---|---|
| Number | Unique number of the milestone. This number is automatically generated. |
| Type | Audit milestone type. The choices are:<br>◦ Scoping<br>◦ Planning<br>◦ Fieldwork<br>◦ Follow up<br>◦ Reporting<br>◦ Closure |
| Name | Name of the milestone. |
| Assignment group | Group responsible for the milestone. The group members must have the sn_audit.user role. |
| Assigned to | Person responsible for working on the milestone. |
| State | State of the milestone. The default state is **Open**. |
| Percent complete | Percentage of milestone completion. When a value is entered in this field, the state changes to **Work in progress**. |
| Parent | Parent engagement of the milestone. |
| Key milestone | Option to mark the milestone as important. |
| Auto complete and close | Option to mark the milestone as close complete when all the associated audit |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | tasks are completed and closed. If this option enabled, then the percent complete is automatically updated as per the number of tasks marked as closed complete. |
| Description | Brief description of the milestone. |
| Schedule | |
| Due date | Expected completion date of the milestone. |
| Completion date | Actual completion date of the milestone. |
| Closed date | Actual close date of the milestone. |
| Activity | |
| Worknotes | Worknotes for the milestone. |
| Additional comments (Customer visible) | Comments related to the milestone, if any. |

6. Save the form.
   The Audit Tasks related list appears.
7. On the Edit Members form, move the required audit tasks from the available audit tasks in the Collection column to the Audit Tasks List column, and then click **Save**.
   The milestone is created.

### Create a milestone from an audit task

Create and track an audit task as a milestone.

**Before you begin**
Role required: sn_audit.manager

**Procedure**

1. Navigate to **All** > **Audit** > **Milestones** > **All Milestones**
2. Open the Milestone that contains the audit task that you want to track.
3. From the Audit Tasks related list, open the audit task you want to track.
4. Click **Track as a Milestone**.
   The milestone is created and the task is added to the milestone.

## Integration of Audit Management with Time Card management

Audit users and audit managers can now use the Time Card Management feature to log and capture hours for engagements and other tasks on an engagement.

The Time Card management feature enables users to submit and track their time for the assigned tasks. With the Time Card Management feature:

- The time card users can record the time worked on a task using time cards and time sheets. They can then submit their time cards and time sheets for approval.
- Time cards and time sheets are routed for approval based on the **Non-project time approver** field in the user time sheet policy. Managers with the time card approver role can also log time and submit the time sheet of their resources.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When you integrate Audit Management with Time Card management, you can report a time card for:

- an engagement
- audit tasks
- issues
- milestones

To use the Time Card management feature integration with GRC Advanced Audit, you must activate the following plugins:

- Project Portfolio Management
- GRC: Advanced Audit

**Note:** You must enable advanced planning for the engagement.

When an audit user logs time using time cards, the time cards are sent for approval based on the approvers defined in the time sheets policy. To learn more about time sheets policy, see Time sheet policy

**Note:** If there's no approver identified or **None** is selected in the **Non-project time approver** field on the time sheet policy assigned to the user, then the users in the **Time card approver** field are able to approve the time cards associated to that engagement. If **User Manager** or **Auto** is selected in the **Non-project time approver** field, then the approvers are not overridden and remain as is. For details on the roles required to approve time cards, see Roles required for Advanced planning capability and Project Portfolio Management integration

To create a time card, see Create a time card.

A user can submit the time cards through the time sheet portal directly without coming to the engagement. To submit a time card, see Submit a time card. To submit a time card from the time sheet portal, see Submit time card from the time sheet portal

### Time cards and rollup of expenses and resources

In the version 12.0.1, release of Audit Management, when an engagement has a project associated with it, after a time card is approved and expense lines are processed, both the **Actual resources** and the **Actual expenses** values roll up on the engagement. Although you can create a time card and log hours before you create a project for an engagement, it is recommended to create a time card after a project is created. This task ensures accurate reporting of the expenses and resources. The Time Cards related list appears on an engagement only after a project is created.

Related topics

Roles required for Advanced planning capability and Project Portfolio Management integration

## Audit observations

Audit observations are the results of an audit. As an important part of the audit report, audit observations represent the results of reviews, analysis, interviews, and discussions.

Audit observations are used to bring significant issues to the attention of audit managers. Observations are logged in the system. For example, if a bank's operations are being audited, then the audit observations are based on evidence about how the bank's

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

operations perform against the audit criteria. During control testing, interviews, and walkthroughs, audit observations are recorded. An audit user can create an observation from an engagement if the engagement is not in the Follow Up or Closed states. An observation can also be created from all types of audit tasks.

After the auditor completes the audit, the auditor then presents the audit observations to the audit managers. By using the audit observations, the auditor can present a summary of problems, discoveries, and recommendations. The audit team reviews the observations to determine if the observation is a reportable issue. The audit team can also determine if the observation can be tracked as a recommendation, an observation, or a best practice.

In its life cycle, an audit observation moves through the following states:

1. Draft
2. Review
3. Respond
4. Finalize
5. Closed

The workflow of an observation is as follows:

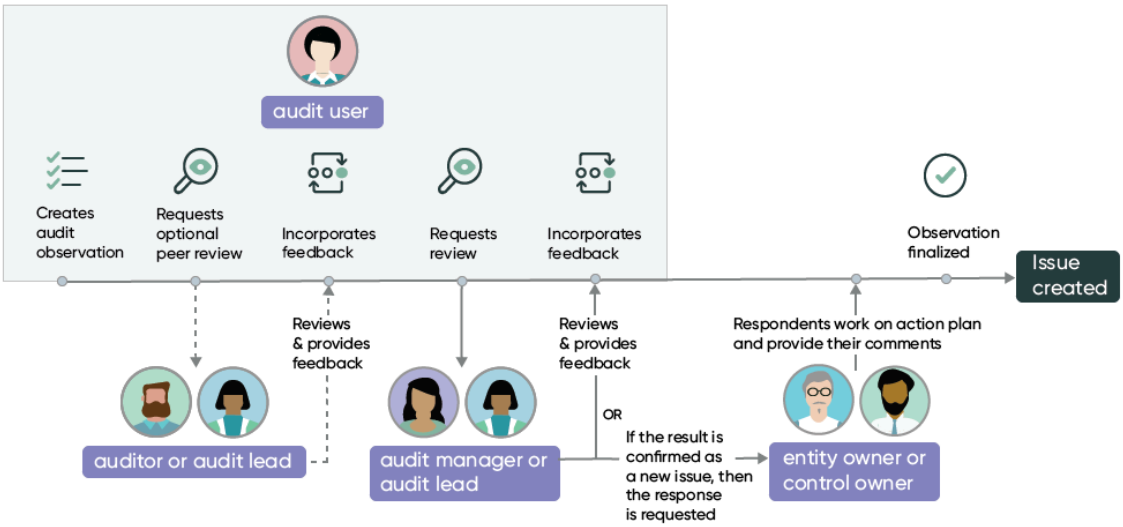
1. An audit user with the role sn_audit.user creates an observation.
2. The observation creator assigns respondents and peer reviewers to the observation. The respondents are the entity owners and control owners. The peer reviewers are the auditors and audit leads of the engagement.
3. The observation creator can request a peer review of the observation. In that case, the following then happens.
   a. The peer reviewer gets a notification to perform the peer review. The peer reviewer can view the task under **Audit** > **Observations** > **My Pending Peer Reviews**.
   b. The peer reviewer completes the review.

   **Note:** When a peer review is requested, the state remains as Draft but the substate changes to the Peer review requested substate.

4. The observation creator can also request a review. The reviewer can be an audit manager or the audit lead.
   a. The reviewer gets a notification to perform the review. The reviewer can view the task under **Audit** > **Observations** > **My Pending Reviews**.
   b. The reviewer can either request a revision of the observation or request a response from the respondent. The reviewer can also provide feedback in the Results section by selecting the appropriate option.
5. If the reviewer requested a response from the respondent, then the respondent responds to the observation by navigating to **Audit** > **Observations** > **My Pending Response**.
6. The observation moves to the Finalize state.
7. The observation is closed and an issue is created.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Audit observations workflow




## Roll up expenses and resources in an engagement

Any audit project has associated costs, budgets, and resources. Roll ups of these costs, budgets, and resources enable the audit manager to view the entire costs and resources in a consolidated manner.

Starting with the new release, a new plugin called Advanced Audit has been introduced in the Audit Management application. When you activate the Advanced Audit plugin and install the Project Portfolio Management application, you can utilize the project management capabilities to automatically create engagement projects.

When an audit plan is created, the audit manager must be able to view the complete expenses and the resources involved in the engagement. Activating the Advanced Audit plugin enables the rollup of the expenses and resources cost of all engagements for a consolidated view. You can also use the advanced planning capabilities to automatically roll up the expenses and resources of each individual engagement to the parent plan of the engagements.

### Project budget rollup

After an engagement project is automatically created, if the user has the it_portfolio_manager role, the user can create a project budget. When a budget is created, the budget cost gets copied over to the **Budgeted expenses** field of the engagement from the engagement project. When you use the advanced planning capabilities to automatically create a plan, the values in the expenses and the resources field are rolled up from the associated engagements and the engagement projects. To allocate a project budget, see Allocate budget to a project. If you allocate a project budget, then the data from the budget cost field gets copied over to the engagement. For example, if you have an engagement where the budget expense is $100. Then, if you create a project budget for the engagement project of this engagement, and enter the budget cost as $200, then the budget expense of $100 in the engagement is overwritten and replaced by $200.

### Actual expenses and resources rollup

If actual effort is updated on an engagement project, then that value gets copied over to actual resources on the engagement. The **Actual resources** and **Actual expenses** both are copied over from the **Actual effort**and **Actual cost** fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Resource plan rollup

With Project Portfolio Management, you can add resource plans and cost plans to an engagement. To learn how to create an engagement with advanced planning, see Create an engagement with advanced planning

After you create a resource plan and it is in the **Allocated** state, all the confirmed and allocated hours from the resource plan are summed up in the planned resources on the engagement project. When a resource plan is created, you cannot manually enter the hours in the **Planned resources** field on the engagement form as the values get automatically rolled up. To manually enter hours in the **Planned resources** field, you must delete the resource plan that you have created.

### Cost plan rollup

If you create an independent cost plan that is not created as a result of a resource plan, then you cannot manually enter values in the **Planned expenses** field on the engagement form. You can still edit the **Planned resources** field.

## Roles required for Engagement project planning for Project Portfolio Management

The advanced planning capability enables integration of Advanced Audit with the Project Portfolio Management (PPM) product. The capability creates an equivalent project for the engagement, and provides planning features that could be used for resource planning, cost planning, and so on, from the engagement project.

### Engagement-project planning features and roles

To understand the roles required for using the engagement-project planning features, see the following table:

**Engagement-project planning features and role requirements**

| Feature | Description | Roles and their scope |
|---|---|---|
| Resource planning | As a resource requester, find the availability of the resources, and create and manage the resource plans for the project and project tasks in the project workspace. For more information, refer to Create and manage resource plans for a project | • Users with at least resource_user role can add resource plans using the **New** button and with it_project_manager role can manage and add new resource plans using the **Manage** button. Users with resource_manager role would be able to confirm and allocate resource plans.<br>• Users with sn_ppm_read or timecard_user or resource_user role would be able to see the resource plans for the engagement project. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Engagement-project planning features and role requirements (continued)**

| Feature | Description | Roles and their scope |
|---|---|---|
| Cost planning | Project cost plans capture the costs of projects. Create a cost plan to specify the unit cost of a cost type for a fiscal period. For more information, refer to Create a project cost plan | • Users with sn_audit.user or sn_audit.manager role and it_project_manager would be able to manage the cost plan. Users with the it_project_manager role can add new cost plans. Users with sn_audit.user or sn_audit.manager and project_manager role would be able to add a new cost plan.<br>• Users with sn_audit.user or sn_audit.manager role and project_manager role would be able to add a new cost plan. Users are suggested to use the it_project_manager role instead of project_manager role by PPM. Users with the it_project_manager role can also add new cost plans. |
| Related links on Engagement project | Users can enter the project budget, move projects, calculate completion estimates for the engagement project using the related links which appear based on the roles and permissions. | • Users need portfolio_manager role to create project budget. If a user role is being added manually, use the it_portfolio_manager role instead of portfolio_manager role.<br>• Users need project_manager role to be able to calculate completion estimates, and move project. If a user role is being added manually, use the it_project_manager role instead of project_manager role. |

Related topics

Roles required for Advanced planning capability and Project Portfolio Management integration

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Roles required for Advanced planning capability and Project Portfolio Management integration

The advanced planning capability enables integration of Advanced Audit with the Project Portfolio Management (PPM) product. The capability creates an equivalent project for the engagement, and provides planning features that could be used for resource planning, cost planning, and so on, from the engagement.

## Engagement planning features and roles

To use the new features of advanced planning capability, users must have the following roles:

**Engagement planning features and role requirement**

| Feature name | Description | Roles and their scope |
|---|---|---|
| Resource Planning | As a resource requester, find the availability of the resources, and create and manage the resource plans for the project and project tasks in the project workspace. For more information, refer to Create and manage resource plans for a project | • Users with sn_audit.manager plus resource_user or resource_manager roles would be able to manage and add resource plans. Users with resource_manager role would also be able to confirm and allocate the resource plans.<br>• Users who already have access to the engagement and also have sn_ppm_read or timecard_user or resource_user roles are able to view the resource plans on the engagement. |
| Cost Planning | Project cost plans capture the costs of projects. Create a cost plan to specify the unit cost of a cost type for a fiscal period. For more information, refer to Create a project cost plan | • Users with sn_audit.user or sn_audit.manager plus it_project_manager roles would be able to manage the cost plans.<br>• Users with sn_audit.user or sn_audit.manager plus project_manager roles would be able to add a new cost plan.<br>**Note:** Users are suggested to use it_project_manager role instead of project_manager role by PPM product. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Engagement planning features and role requirement (continued)**

| Feature name | Description | Roles and their scope |
|---|---|---|
| | | • Users who already have access to the engagement and also have sn_ppm_finance_read or demand_manager or program_manager or portfolio_manager or project_manager roles are able to view the cost plans for the engagement. |
| Resource allocations | After resource requesters create a resource plan, resource managers can confirm the resources to move the plan to the Confirmed state. Resource managers can then allocate resources to the plan and move it to the Allocated state.<br><br>Based on calendar and schedule information, resource managers view resource availability and select the resources under their management that can be confirmed and allocated to specific tasks. For more information, refer to Resource allocation | • Users need both pps_resource and sn_audit.user or sn_audit.external_auditor roles to be added to the auditors field on the engagement from the resource plan.<br>• Users need pps_resource role to be added as resources to the resource plans. |
| Time card reporting | You can log hours in a time card for an engagement and other tasks on an engagement. If there is a project associated with an engagement, then the actual expenses and actual resources values roll up. To create a time card, see Create a time card. | • Users need timecard_user role to create a time card.<br>• Users who already have access to the engagement, audit tasks, milestones, issues and also have sn_ppm_read or timecard_approver or timecard_admin roles will be able to view all the time cards on the engagement, audit tasks, milestones, and issues.<br>• Users who already have access to the engagement, audit tasks, milestones, and |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Engagement planning features and role requirement (continued)**

| Feature name | Description | Roles and their scope |
|---|---|---|
| | | issues and also have the timecard_user role will only be able to view the time cards that they have reported on the engagement, audit tasks, milestones, and issues.<br>• Users need timecard_approver role to approve a submitted time card. The time sheet policy assigned to the user governs the approval process. |

Related topics

Roles required for Engagement project planning for Project Portfolio Management

# Business Continuity Management

ServiceNow® Business Continuity Management application gives your organization the capability to continue to deliver products and services at an acceptable level when a disruptive incident occurs. The ongoing activities of this application are aimed to reduce the operational risks and improve your organizational ability to respond, react, and recover from issues and disruptions.

## Business Continuity Management overview

The Business Continuity Management product provides a framework to perform continuous management activities. The Business Continuity Management application helps your organization to achieve the following objectives:

- Establish a clear governance structure.
- Define a consistent classification of business processes, interdependencies, and recovery objectives based on impact analysis and risk to the business.
- Develop and provide continuous improvement to the business continuity plans.
- Identify, analyze, and manage process continuity during and following a disruptive event.

For more information on Business Continuity Management, see Exploring Business Continuity Management.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Get started

| Explore | Configure | Manage |
|---|---|---|
|  |  |  |
| Explore key features of BCM | Set up the BCM application | Manage your business continuity tasks |
| **Notify** | **Classic workspace** | **Reference** |
|  |  |  |
| Send emergency notifications with Everbridge | Use BCM Classic workspace | Components installed with BCM |

### Support for Business Continuity Management UI Builder Workspace

Starting with the Utah release, you can configure the Business Continuity Management application in the UI Builder Workspace. UI Builder is a Web user interface builder to build or customize your Workspace pages by using Next Experience Components.

For more information on the next generation of the user interface, see Next Experience UI.

For information on the UI Builder administrative tasks in BCM, see Setup for the UI Builder.

For instructions on how to configure your business continuity tasks in BCM UIB Workspace, see Managing business continuity workflow tasks in BCM UIB Workspace.

**Note:** Starting with the Utah release, the BCM classic Workspace is being prepared for future deprecation. It will be hidden from the navigation on the new instances but it will continue to be supported. The BCM UIB Workspace provides the latest experience for this functionality.

### Troubleshoot and get help

- Ask or answer questions in the GRC community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support
- Developer training
- Developer documentation

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Exploring Business Continuity Management

Learn how you can use the Business Continuity Management application to manage your business continuity tasks using predefined templates and workflows.

## Business Continuity Management overview

The Business Continuity Management application provides a framework to perform continuous management activities such as business impact analysis, business continuity planning, exercise management, and crisis management. The structured workflows in the Business Continuity Management application improve your organizational ability to respond to the issues and recover quickly from the disruptions.

## Business Continuity Management workflow

A typical workflow in the Business Continuity Management application involves the following steps for managing your business continuity tasks:

1. An administrator downloads the Business Continuity Management application from ServiceNow Store.
2. The BCM administrator sets up the Business Continuity Management application and the templates for performing the business continuity activities.
3. The BCM program manager or business impact analysis (BIA) administrator creates a business impact analysis to determine the impact of a disruption on the business processes and IT applications. The BIA administrator also focuses on the consequences of incidents and estimates the time of recovery to resume normal business operations.
4. The BCM program manager or BCM lead reviews the assessments and approves the business impact analysis.
5. The BCM program manager or business continuity plan (BCP) administrator creates a business continuity plan and adds the relevant assets, scope, documentation, related plans, recovery teams, loss scenarios, and recovery tasks to it. The BCP administrator then sends an approval request to the BCM lead to review and approve the business continuity plan.
6. The BCM program manager creates exercise events, tracks the assets and their dependencies, and approves the exercise events.
7. The BCM program manager responds to the crisis events, tracks the assets and their associated dependencies, and manages the recovery tasks to mitigate the negative impact of a disruption.
8. The BCM program manager manages the alerts from the Crisis map interface and initiates the response workflows to minimize the downtime.
9. The BCM administrator or BCM program manager sends the emergency notifications in Everbridge notifications system and notifies the stakeholders about the crisis alerts.

## Business Continuity Management benefits

The Business Continuity Management application provides the following benefits:

| Benefits | Features | Users |
|---|---|---|
| Manage your business continuity activities from the interactive dashboard in the Home page. | Home page view | BCM program manager |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Benefits | Features | Users |
|---|---|---|
| Monitor your individual and team tasks from a single dashboard in the **My tasks** view. | My tasks page view | BCM program manager |
| Assess your critical business services and IT applications by creating a business impact analysis. | Create a business impact analysis | BCM program manager or BIA administrator |
| Prepare a business continuity plan with a response strategy and get it reviewed by the BCM leads and program managers. | Create a business continuity plan | BCM program manager or BCP administrator |
| Finalize your business continuity plan by continuously testing and exercising an event. | Create an exercise | BCM program manager or BCM planner |
| Respond to an actual crisis event and manage the associated event tasks. | Start a crisis event | BCM program manager or BCM planner |
| Respond to the alerts in Crisis map and set the recovery tasks into action to manage the alerts. | Manage the alerts in Crisis map | BCM administrator or BCM program manager |
| Notify the stakeholders about the crisis alerts by sending emergency notifications in Everbridge. | Sending notifications with Everbridge in BCM Configurable Workspace | BCM administrator or BCM program manager |

## BCM Configurable Workspace

Starting with version 5.x.x, the Business Continuity Management application supports BCM Configurable Workspace. You can perform your business continuity tasks with an intuitive functionality in BCM Configurable Workspace.

## Enhancements in BCM Configurable Workspace

BCM Configurable Workspace (also known as Business Continuity Workspace) offers an enhanced and simplified user experience for its users. The BCM application users can take advantage of the following enhancements in BCM Configurable Workspace over BCM classic Workspace:

1. Manage the crisis events, business impact analysis, planning, and exercises from an interactive dashboard in the Home page.
2. Monitor your individual and team tasks in the My tasks page and act on your pending tasks quickly.
3. Respond to the alerts in Crisis map and manage the recovery tasks effectively.
4. Visualize 360-degree relationship data for your business impact analysis, planning, exercises, and crisis events records and get a complete overview of all dependencies.

**Note:**

Starting with the Utah release, the BCM classic Workspace is being prepared for future deprecation. The Business Continuity Workspace in the classic Workspace is automatically updated to point to BCM Configurable Workspace.

**Note:** For information on BCM classic Workspace, see Using BCM classic Workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Configurable and role-driven Workspace

BCM Configurable Workspace is configurable and role-driven. It is customized and unique for each user or role in your organization. You can log in with specific user roles to perform different functions and the user interface views differ from each other.

For more information on the user roles in the BCM application, see Components installed with Business Continuity Management.

For more information on the store apps to install and activate the application, see Business Continuity Management and the ServiceNow Store.

## Users of the BCM application

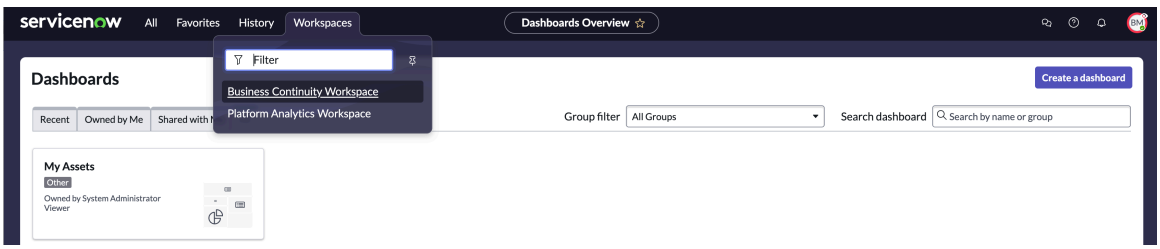
The BCM application is the central workbench for the following types of users:

- BCM administrators
- BCM managers
- BCM planners
- BCM contributors
- BCM viewers
- Business users
- IT application owners

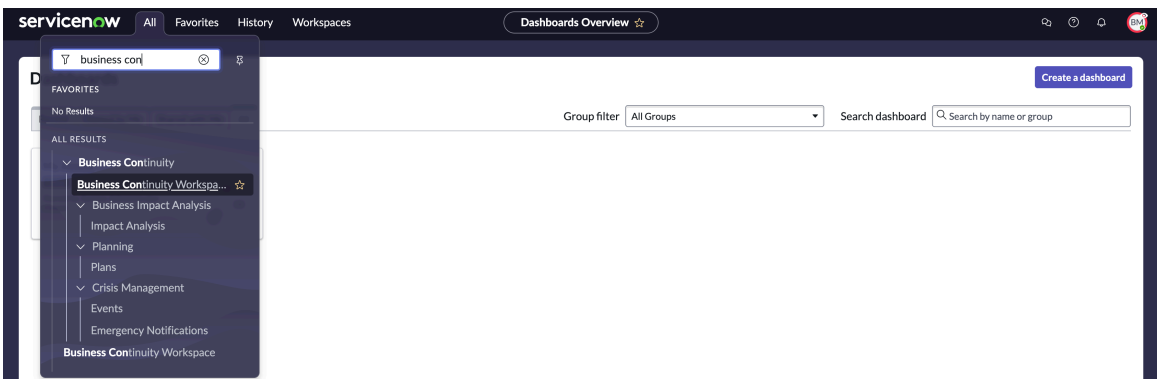
## Navigating to BCM Configurable Workspace

When you log in to the Business Continuity Management application with a specific user role, you can navigate to the Business Continuity Workspace by using one of the following options:

- First option: Navigate to **Workspaces > Business Continuity Workspace** in the application instance as shown in the following example.




- Second option: Navigate to **All > Business Continuity > Business Continuity Workspace** in the application instance as shown in the following example.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** The Business Continuity Workspace in the classic Workspace view is automatically updated to navigate to BCM Configurable Workspace.

## Icons in Business Continuity Workspace

When you launch Business Continuity Workspace, you can view the following icons in the side bar of the Workspace view.

- Home page: Displays your business continuity tasks in a single pane view.
- Tasks page: Displays an overview of the tasks for the logged-in user. For more information, see My tasks page view.
- Lists: Displays the count and status of the business impact analysis, planning, exercise, and crisis event records. For more information, see List view.
- Crisis map: Displays the real-time threat alerts from different locations in a map view. For more information, see Crisis map view.

## Managing functional components in BCM Configurable Workspace

You can manage the following functional components of the BCM application in BCM Configurable Workspace:

Business impact analysis

Performing a business impact analysis helps you to identify high risk assets and determine the impact of disruption on your critical business functions or services. By analyzing the impact, you can estimate the time of recovery to resume business and also focus on the consequences of incidents and disruptions.

For information on creating a business impact analysis, see Business impact analysis. For information on the structured workflow tasks for business impact analysis, see Structured workflows for Business Impact Analysis in BCM UIB Workspace.

Business continuity planning

Planning your business continuity tasks enables you to develop continuity and recovery plans for critical business processes and IT functions. Disaster recovery enables you to protect, recover, and restore the organizational critical data and its technology systems. You can also develop a business continuity strategy for each activity.

For information on creating a business continuity plan, see Business continuity planning. For information on the structured workflow tasks for business continuity planning, see Structured workflows for Business Continuity Planning in BCM UIB Workspace.

Exercise management

Creating an event to exercise the plan in a simulated crisis helps you to validate your business continuity plans by continuous testing. You can then improve the effectiveness of the plans and usability during a simulated crisis.

For information on the exercise events, see Exercises. For information on the structured workflow tasks for exercise management, see Structured workflows for Exercise Management in BCM UIB Workspace.

Crisis management

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Managing an actual crisis event helps you to mitigate the negative impact of a disruption to the business system. You can then prioritize the actions and apply the right strategy to minimize the downtime.

For information on the crisis events, see Crisis events. For information on the structured workflow tasks for crisis management, see Structured workflows for Crisis Management in BCM UIB Workspace.

**Note:** For setting up Business Continuity Management, see General administration setup for BCM.

### Home page view

The Home page in Business Continuity Workspace serves as the landing page of the BCM application.

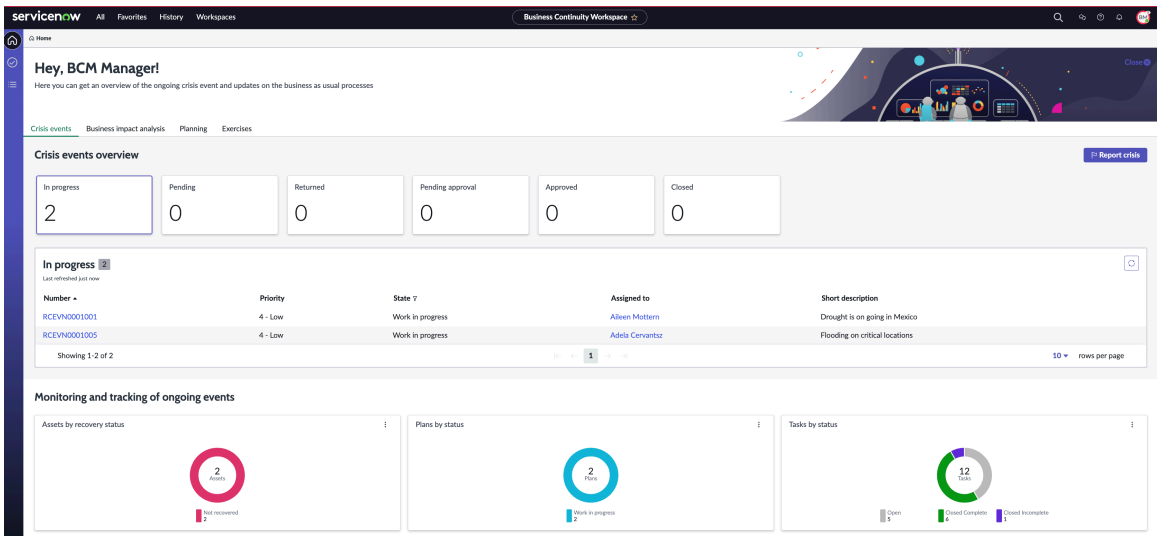
## Home page in Business Continuity Workspace

The Home page in Business Continuity Workspace provides an overview of the BCM functional components in an interactive dashboard. The visualizations help the Workspace users to know the status of their tasks and act on them in an organized manner. The Home page consists of the following tabs:

- **Crisis events**
- **Business impact analysis**
- **Planning**
- **Exercises**

## Crisis events tab

The **Crisis events** tab in the Home page displays various cards that offer information on the crisis events. You can review the crisis events in various states, details of the selected crisis events, and monitoring and tracking of the crisis events. The following example shows the cards in the **Crisis events** tab.




See the following table for the description of the cards in the **Crisis events** tab:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Cards in the Crisis events tab

| Card | Description |
|---|---|
| Crisis events overview | Overview of the crisis events in different states. You can view the details of the crisis events in the following states:<br>In progress<br>Number of the crisis events that are in the **In progress** state.<br>Pending<br>Number of the crisis events that are in the **Pending** state.<br>Returned<br>Number of the crisis events that are in the **Returned** state.<br>Pending approval<br>Number of the crisis events that are in the **Pending approval** state.<br>Approved<br>Number of the crisis events that are in the **Approved** state.<br>Closed<br>Number of the crisis events that are in the **Closed** state. |
| Details of the selected event card | Details of the crisis events for the selected state of the card. For example, if you selected **In progress** in **Crisis events overview**, then details of the crisis events that are in the **In progress** state are displayed in this panel. You can view the following details on the crisis events:<br>Active<br>State of the crisis event. The state can be **True** or **False**. You can select the link to open the crisis event record.<br>Activity due<br>Activity that is due on the crisis event.<br>Participants<br>Participants of the crisis event.<br>Approval<br>Approval information for the crisis event.<br>Approval history |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Cards in the Crisis events tab (continued)**

| Card | Description |
|---|---|
| | Approval history of the crisis event.<br>Assigned to<br>Name of the assignee responsible to respond to the crisis event. When you select the assignee name in the column, it opens the record form where the following tabs are displayed:<br>• **Details**<br>• **Roles**<br>• **Groups**<br>• **Delegates**<br>Assignment group<br>Assignment group for the crisis event.<br>Business duration<br>Business duration of the crisis event.<br>Service<br>Service impacted due to the crisis event. |
| Monitoring and tracking of ongoing events | Graphical representation of all crisis events. You can filter the information based on their associated assets, plans, and tasks in a pie chart format:<br>Assets by recovery status<br>Shows the number of the assets by their recovery status for ongoing events. The following details are displayed on the asset in a pie chart:<br>• Not recovered<br>• Recovered<br>The example in the image shows that out of the total 18 assets, 17 assets are not yet recovered and one asset is recovered.<br>Plans by status<br>Shows the plans by the following status of the ongoing events: |

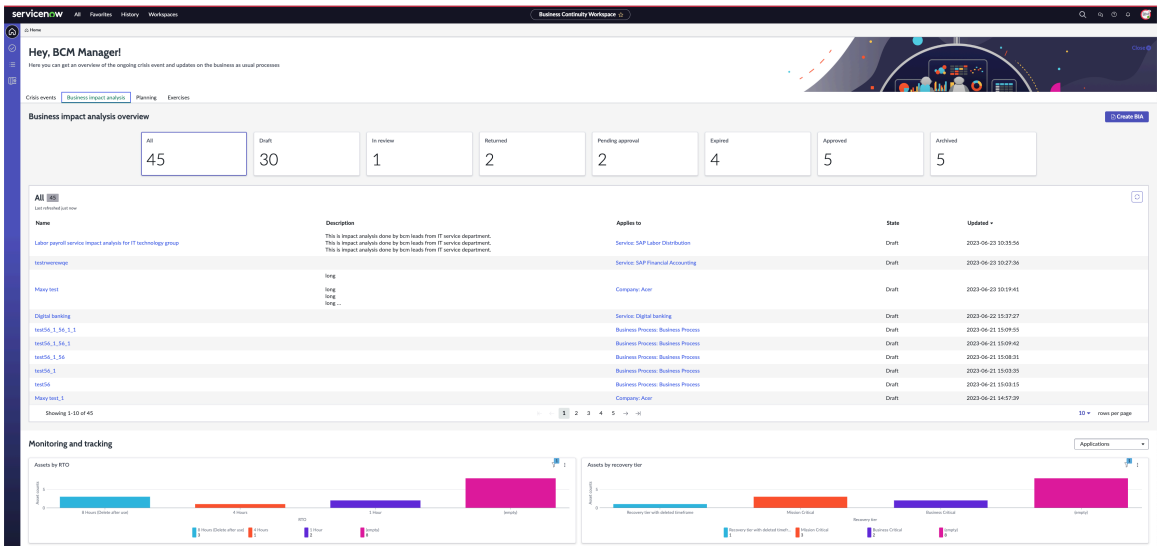
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Cards in the Crisis events tab (continued)**

| Card | Description |
|---|---|
| | • Pending<br>• Work in Progress<br>• Closed Complete<br><br>Tasks by status<br>Shows the tasks by the following status of the ongoing events:<br>• Open<br>• Pending<br>• Closed Incomplete<br>• Closed Complete<br>• Closed Skipped |
| **Report crisis** action button | Action button to report a crisis and create a crisis event from the **Crisis events** tab. When you select **Report crisis**, it launches the **Create New Event** form where you can fill in the details of the crisis event. |

## Business impact analysis tab

The **Business impact analysis** tab in the Home page displays various cards that offer information on the business impact analyses. You can review the business impact analyses in various states, details of the selected analyses, and monitoring and tracking of the analyses. The following example shows the cards in the **Business impact analysis** tab.




See the following table for the description of the cards in the **Business impact analysis** tab:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Cards in the Business impact analysis tab

| Card | Description |
|---|---|
| Business impact analysis overview | Overview of the business impact analysis in different states. You can view the details of the business impact analysis in the following states:<br>All<br>Total number of the business impact analyses in the BCM application.<br>Draft<br>Number of the business impact analyses in the **Draft** state.<br>In review<br>Number of the business impact analyses in the **In review** state.<br>Returned<br>Number of the business impact analyses in the **Returned** state.<br>Pending approval<br>Number of the business impact analyses in the **Pending approval** state.<br>Expired<br>Number of the business impact analyses in the **Expired** state.<br>Approved<br>Number of the business impact analyses in the **Approved** state.<br>Archived<br>Number of the business impact analyses in the **Archived** state. |
| Details of the selected business impact analysis card | Details of the business impact analyses for the selected state of the card. For example, if you selected **In progress** in **Crisis events overview**, then details of the business impact analyses that are in the **In progress** state are displayed in this panel. You can view the following details on the business impact analyses in a tabular format:<br>Name<br>Name of the business impact analysis.<br>Description<br>Description of the business impact analysis. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

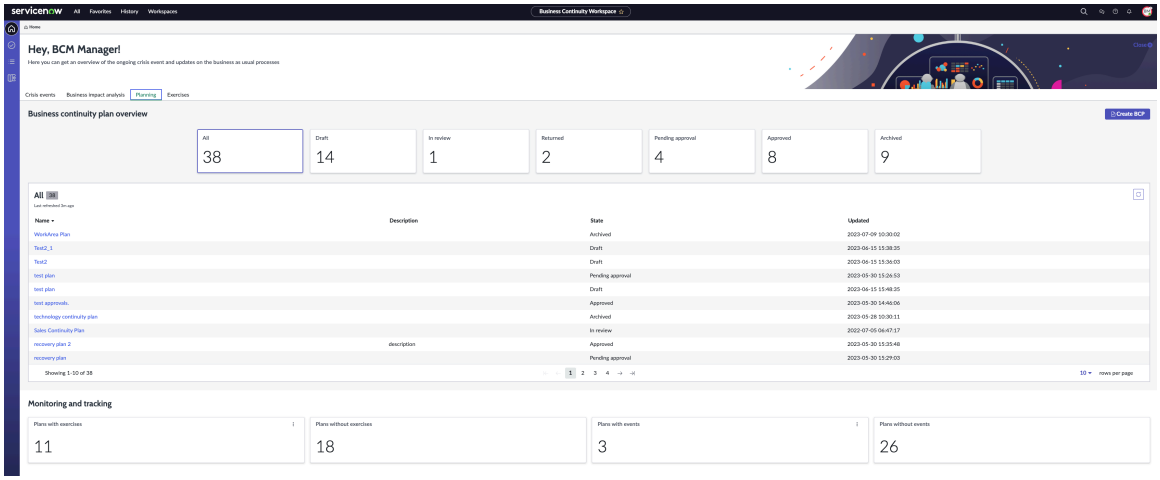
**Cards in the Business impact analysis tab (continued)**

| Card | Description |
|---|---|
| | Applies to<br>Service, process, or company that the business impact analysis applies to.<br>State<br>State of the business impact analysis.<br>Updated<br>Date and time when the business impact analysis gets updated. |
| Monitoring and tracking of ongoing business impact analyses | Graphical representation of all business impact analyses for their assets in a pie chart format:<br>Assets by RTO<br>Shows the number of the assets that have different recovery time objectives (RTO). The image shows an example of three assets that have an RTO of 8 hours and one asset that has an RTO of 4 hours.<br>Assets by recovery tier<br>Shows the number of assets that have different recovery tiers. The image shows an example of three assets that have mission critical recovery tiers and two assets that have business critical recovery tiers. |
| **Create BIA** action button | Action button to create a business impact analysis from the **Business impact analysis** tab. When you select **Create BIA**, it launches the **Create New Impact Analysis** form where you can fill in the details of the business impact analysis. |

## Planning tab

The **Planning** tab in the Home page displays various cards that offer information on the business continuity plans. You can review the business continuity plans, details of the selected plans, and monitoring and tracking of the plans. The following example shows the cards in the **Business continuity plan** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




See the following table for the description of the cards in the **Planning** tab:

### Cards in the Planning tab

| Card | Description |
|---|---|
| Business continuity plan overview | Overview of the business continuity plans in different states. You can view the business continuity plans in the following states:<br>All<br>All business continuity plans in the BCM application.<br>Draft<br>Business continuity plans that are in the **Draft** state.<br>In review<br>Business continuity plans that are in the **In review** state.<br>Returned<br>Business continuity plans that are in the **Returned** state.<br>Pending approval<br>Business continuity plans that are in the **Pending approval** state.<br>Approved<br>Business continuity plans that are in the **Approved** state.<br>Archived<br>Business continuity plans that are in the **Closed** state. |
| Details of the selected business continuity plans card | Details of the business continuity plans for the selected state of the card. For example, if you selected **In progress** in **Business continuity plan overview**, then details of the |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

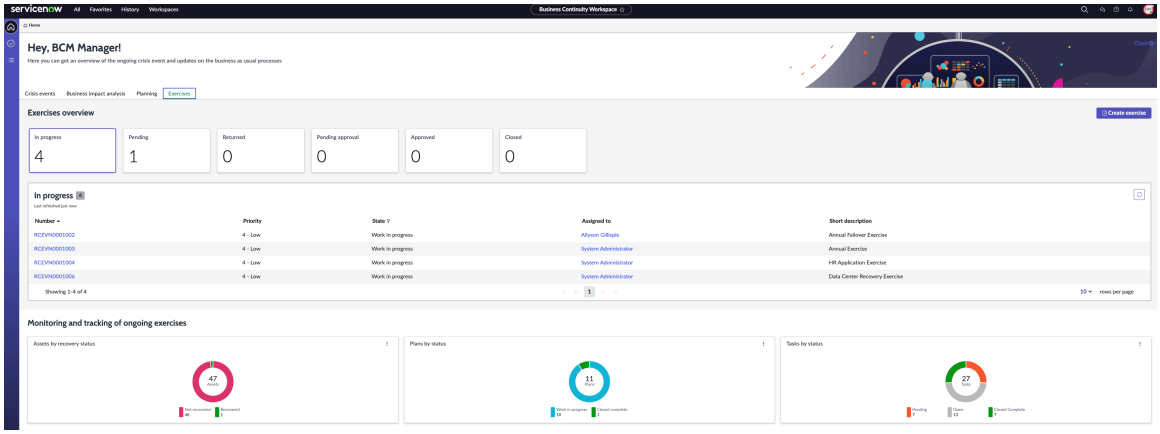
**Cards in the Planning tab (continued)**

| Card | Description |
|---|---|
| | business continuity plans that are in the **In progress** state are displayed in this panel. You can view the following details on the business impact analyses in a tabular format:<br>Name<br>Name of the business continuity plan.<br>Description<br>Description of the business continuity plan.<br>State<br>State of the business continuity plan.<br>Updated<br>Date and time when the business continuity plan gets updated. |
| Monitoring and tracking | Graphical representation of all the active business continuity plans in a pie chart format:<br>Plans with exercises<br>You can select the card to view the plans with exercises.<br>Plans without exercises<br>You can select the card to view without exercises.<br>Plans with events<br>You can select the card to view the plans with events.<br>Plans without events<br>You can select the card to view the plans without events. |
| **Create BCP** action button | Action button to create a business continuity plan from the **Planning** tab. When you select **Create BCP**, it launches the **Create New Plan** form where you can fill in the details of the business continuity plan. |

## Exercises tab

The **Exercises** tab in the Home page displays various cards that offer information on the exercise events. You can review the exercise events in various states, details of the selected exercise events, and monitoring and tracking of the exercise events. The following example shows the cards in the **Exercises** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




See the following table for the description of the cards in the **Exercises** tab:

### Cards in the Exercises tab

| Card | Description |
|---|---|
| Exercises overview | Overview of the exercise events in different states. You can view the details of the exercise events in the following states:<br>In progress<br>Exercise events that are in the **In progress** state.<br>Pending<br>Exercise events that are in the **Pending** state.<br>Returned<br>Exercise events that are in the **Returned** state.<br>Pending approval<br>Exercise events that are in the **Pending approval** state.<br>Approved<br>Exercise events that are in the **Approved** state.<br>Closed<br>Exercise events that are in the **Closed** state. |
| Overview of the exercises for the selected state | Details of the exercise events for the selected state of the card. For example, if you selected **In progress** in **Exercises overview**, then details of the exercise events that are in the **In progress** state are displayed in this panel. You can view the following details on the exercise events in a tabular format:<br>Active |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Cards in the Exercises tab (continued)**

| Card | Description |
|---|---|
| | State of the exercise event. The state can be **True** or **False**. You can select the link to open the exercise event record.<br>Activity due<br>Activity due on the exercise event.<br>Participants<br>Participants of the exercise event.<br>Approval<br>Approval information on the exercise event.<br>Approval history<br>Approval history of the exercise event.<br>Assigned to<br>Name of the assignee responsible for the crisis event. When you select the assignee name in the column, it opens the record form where the following tabs are displayed:<br>• **Details**<br>• **Roles**<br>• **Groups**<br>• **Delegates**<br>Assignment group<br>Assignment group for the exercise event.<br>Business duration<br>Business duration for the exercise event.<br>Service<br>Service for the exercise event. |
| Monitoring and tracking of ongoing exercises | Graphical representation of all active exercises in a pie chart format:<br>Assets by recovery status<br>Shows the number of the assets by the recovery status for ongoing events. The following |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Cards in the Exercises tab (continued)**

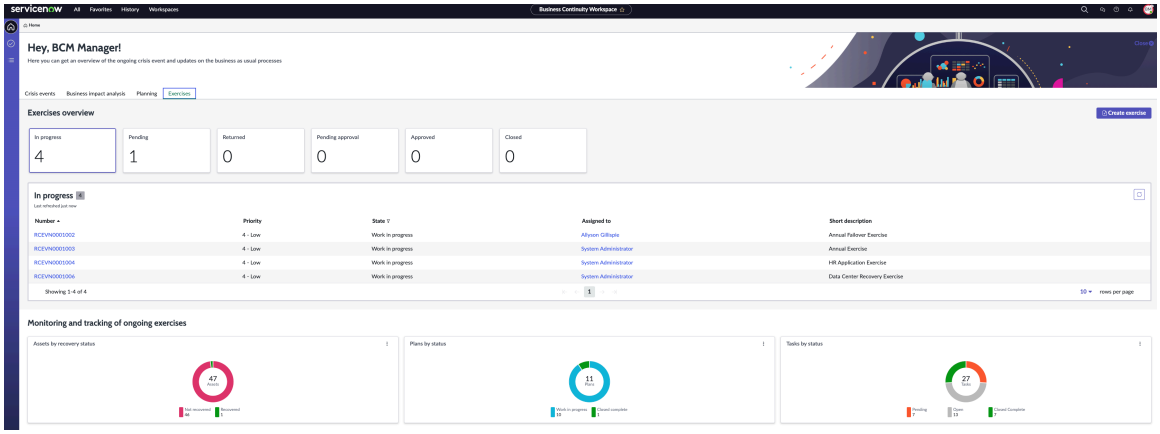
| Card | Description |
|---|---|
| | details are displayed on the asset in a pie chart:<br>• Not recovered<br>• Recovered<br><br>The example in the image shows that out of the total 18 assets, 17 assets are not recovered and one asset is recovered.<br>Plans by status<br>Shows the plans by the following status of the ongoing events:<br>• Pending<br>• Work in Progress<br>• Closed Complete<br><br>Tasks by status<br>Shows the tasks by the following status of the ongoing events:<br>• Open<br>• Pending<br>• Closed Incomplete<br>• Closed Complete<br>• Closed Skipped |
| **Create exercise** action button | Action button to create an exercise event from the **Exercises** tab. When you select **Create exercise**, it launches the **Create New Event** form where you can fill in the details of the exercise event. |

## Home page views for BCM Manager and BCM Planner

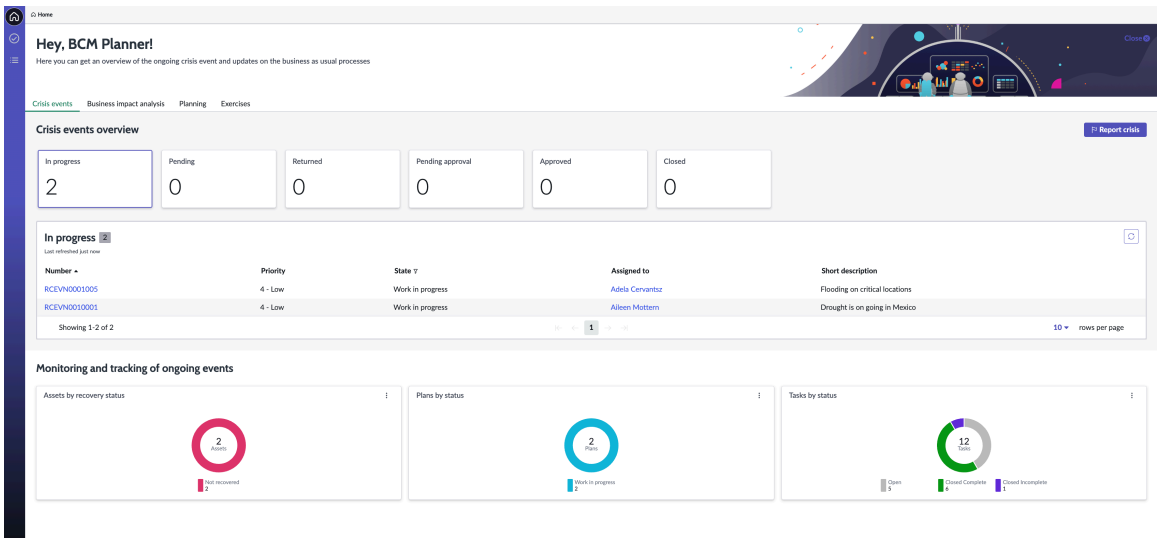
When you log in to the BCM application, the Home page view is displayed according to your user role, responsibilities, and the assigned tasks.

A typical Home page view for a BCM manager is shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




A typical Home page view for a BCM planner is shown in the following example.



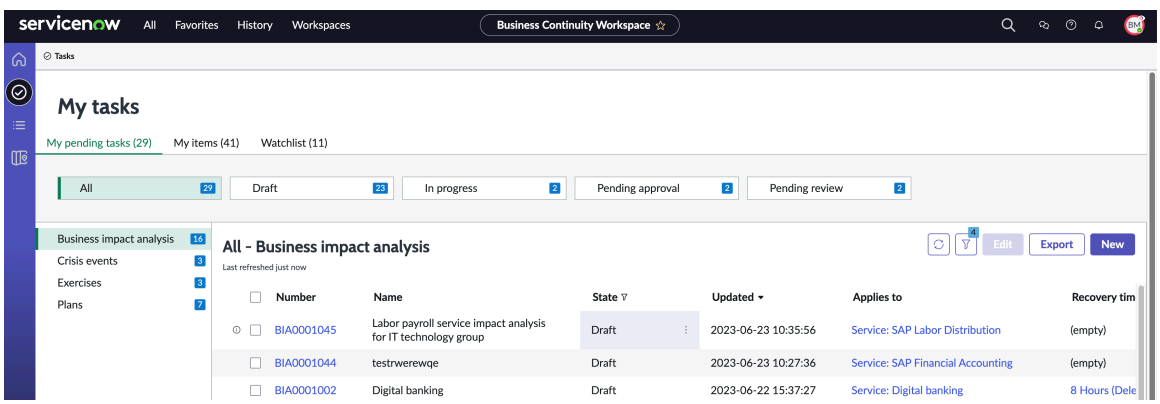

For information on the tabs and their associated actions in the Home page, see Home page view.

## My tasks page view

My tasks page displays a single-pane view of your pending tasks, tasks assigned to your user group, and the tasks that are on your watchlist.

## Tabs in the Tasks page

The Tasks page displays the assigned tasks for the logged-in user in different tabs as shown in the following example.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Tasks page in BCM UIB Workspace displays the following tabs:

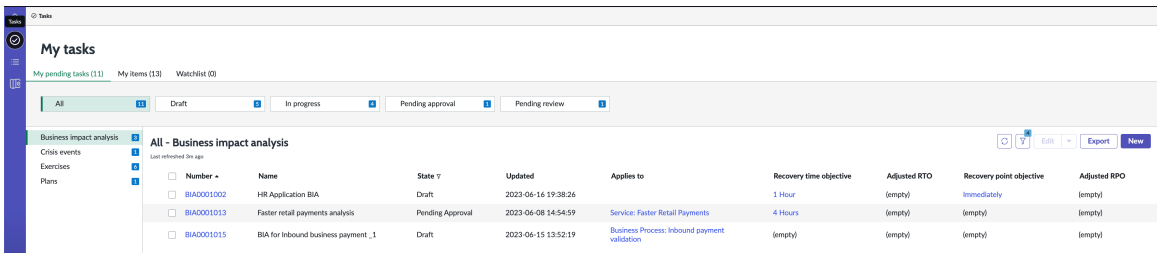
- **My pending tasks**: Displays an overview of the pending tasks that are assigned to you and the tasks that require an action from you. You can filter your pending tasks by using the following types of the states:
  - All
  - Draft/New
  - In progress
  - Needs my approval
  - Needs my review
  - Overdue
  - Pending response

  **Note:** The data displayed in the Tasks page is based on the roles of the users.

- **My items**: Displays a list of the tasks that are assigned to the logged-in user.

- **Watchlist**: Displays a list of the tasks for which you are on the watchlist. When a task is approved or completed, you receive a notification on the **Watchlist** tab.

A typical My tasks page for a logged-in user is shown in the following example.




For more information on the My tasks page configurations module in the application, see My tasks page configurations.

**Note:** On the **My pending tasks**, **My items**, and **Watchlist** tabs, you can only view the records that are in-progress. The closed and canceled records are not displayed on these tabs. You can view the closed and canceled records in their respective forms in BCM UIB Workspace.

If you have the BCM administrator role, you can customize BCM UIB Workspace by updating the Tasks page configurations module. To update the Tasks page configurations, you can navigate to **All > General administration > My tasks page configuration** in your instance.

If you have the BCM manager or BCM user roles, you can also get relevant recommendations on your business continuity tasks on the Home page.

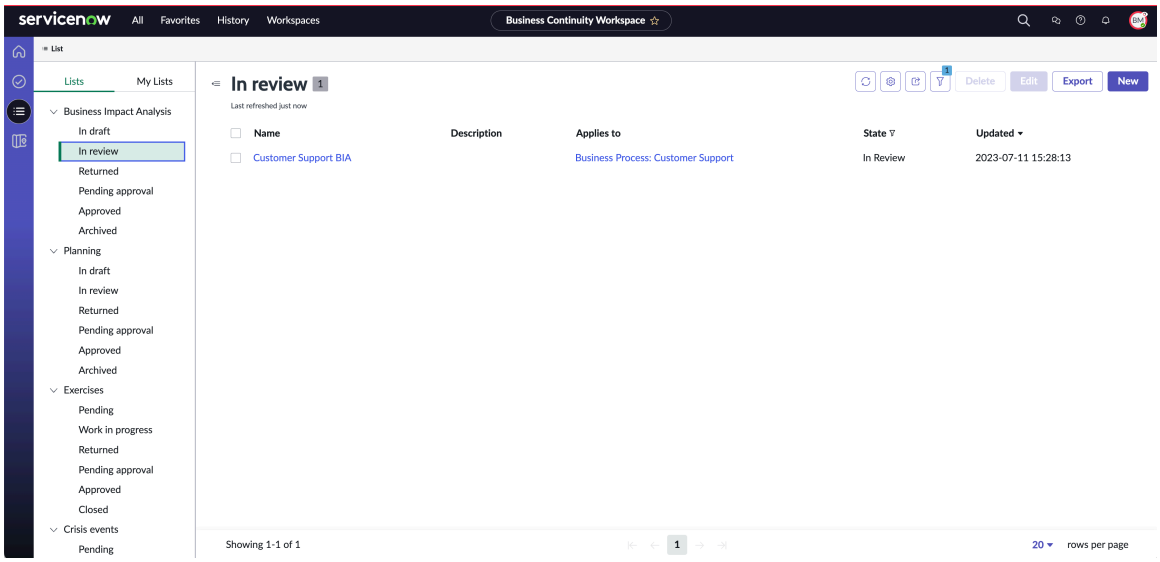
To view more information on the Tasks Page Configuration, see Update the Tasks Page Configuration record.

### List view

The List view in BCM UIB Workspace displays the scope of all BCM functional components and their key metric information.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use the List view to know the count and status of the business impact analysis, planning, exercise, and crisis event records. A typical List view in BCM UIB Workspace is shown in the following example.




The records from each group are listed according to their current state and the record details are configurable. You can create a record by selecting **New**. You can select the link of a record in the **Name** column and view its details.

Use the List view in BCM UIB Workspace to complete the following business continuity tasks:

- Assess the impact of a possible disruption on your business services, processes, and applications. For more information on performing a business impact analysis, see Business impact analysis.
- Create business continuity plans to mitigate the risk at the time of an event. For more information on managing your business continuity planning tasks, see Business continuity planning.
- Create an event to exercise the plan in a simulated crisis. For more information on exercising an event, see Exercises.
- Apply the plan in an actual crisis. For more information on managing a crisis event, see Crisis events.

For information on managing business continuity tasks in BCM UIB Workspace, see Managing business continuity workflow tasks in BCM UIB Workspace.

## Monitoring 360° relationship data for a record

You can monitor the 360° relationship data for your business impact analysis, planning, exercises, and crisis events records. You can also get an overview of the dependencies for each record.

The configurations for the 360° view are stored in **360° View Configurations** > **Configure 360° Views**. If you have the BCM administrator role, you can configure the relationships for the records in **360° View Configurations** > **Relationship Registries**.

For information on configuring 360° relationship registries and views, see Configure 360° relationship registries and views.

For information on how to view 360° relationships of a business impact analysis, see Visualize the 360° relationships for a business impact analysis.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For information on how to view 360° relationships of a business continuity plan, see Visualize the 360° relationships for a business continuity plan.

For information on how to view 360° relationships of an exercise or crisis event, see Visualize the 360° relationships for an exercise and crisis event.

### Crisis map view

When you install the GRC: Crisis map application in your instance, you can view the Crisis map icon in the List view. You can integrate the Crisis map application with BCM and analyze real-time threat alerts from different locations in a map view. You can then take remedial actions and manage the crisis events from Business Continuity Workspace.

## Panels displayed in Crisis map

The Crisis map application consists of the following panels:

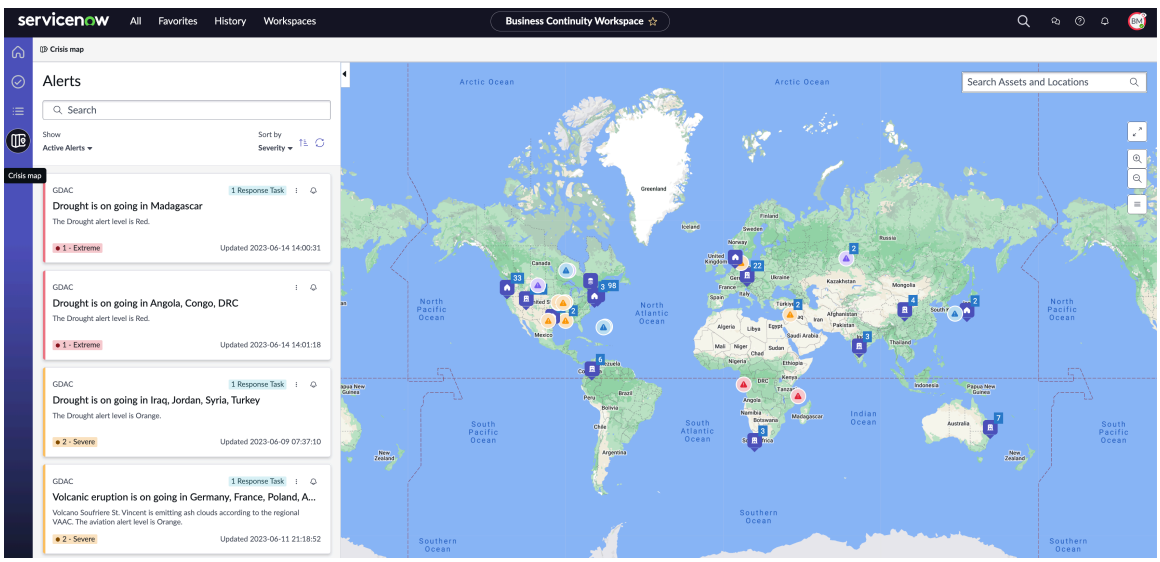
- Alerts panel
- Map view with the locations of the alerts

**Note:**

To enable the search functionality in Crisis map, you must set the *sn_bcm_map.use_google_places_lib* system property. For more information on setting the property, see Properties installed with Business Continuity Management.

To enable Crisis map functionality in the GRC: Crisis map application, you must set up Google maps. For more information, see Set up Google Maps API.

A typical view of the Crisis map application is shown in the following example.




For more information on the feeds, alerts, and events in Crisis map, see Crisis map interface.

## Tasks for a BCM administrator

If you are the BCM administrator, you must perform the following setup tasks for Crisis map:

- Enable threat feed integrations that are provided by the base system.
- Configure additional threat feeds in to the Crisis Management application. The configurations alert the crisis managers about the threats and aids them to take an appropriate action on time.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information on the setup tasks for Crisis map, see Setup for Crisis map in the configuration section.

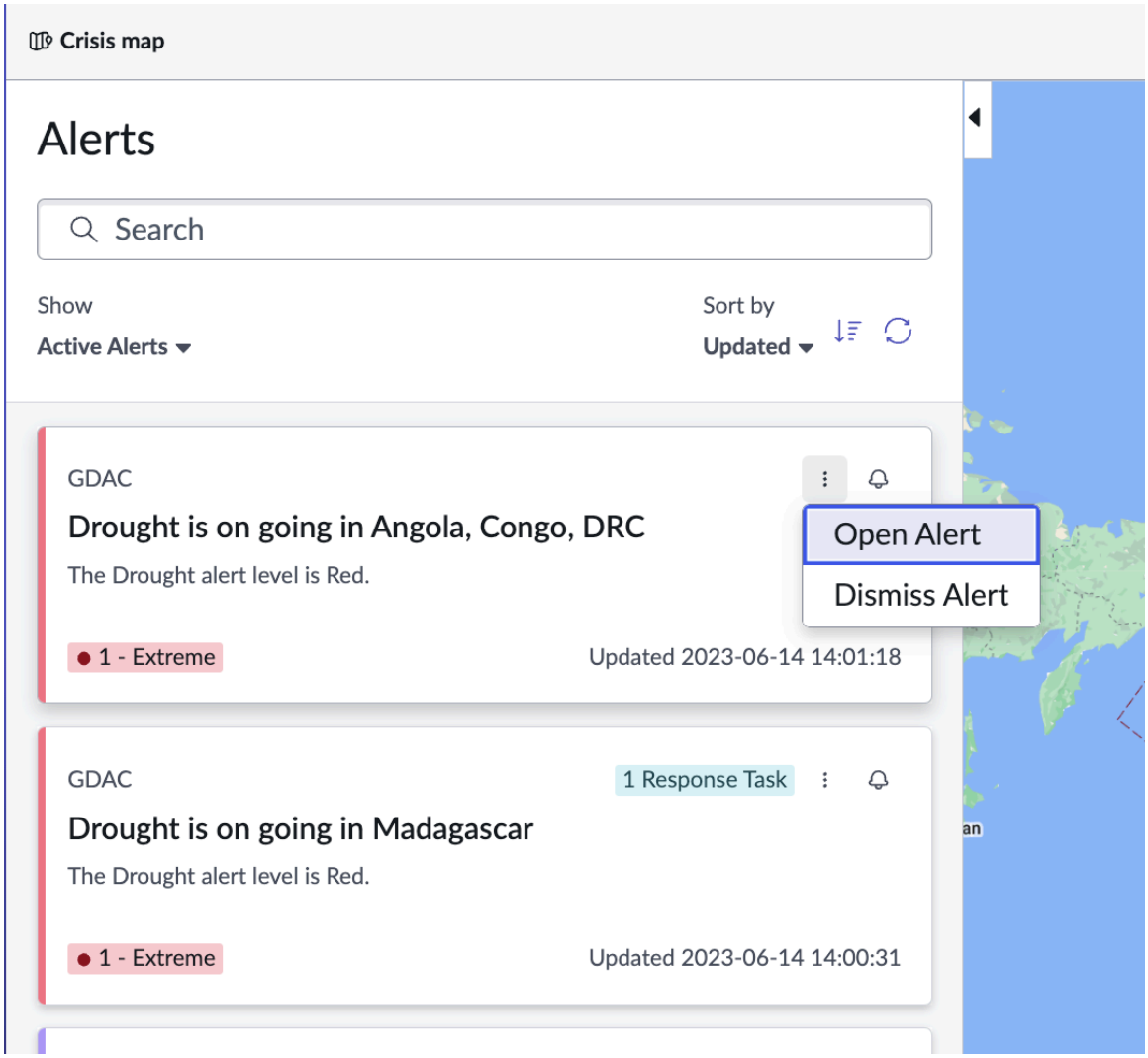
## Alerts panel in Crisis map

The **Alerts** panel in Crisis map displays the following details:

- **Search field**: You can search for an alert by using specific keywords.
- **Show**: You can select this option to display the following types of alerts:
  - **Active Alerts**
  - **Dismissed Alerts**
- **Sort by**: You can select this option to sort the alerts. Select one of the following options:
  - **Severity**: Select this option to sort and display the alerts based on their severity such as **Extreme** or **Severe**.
  - **Created**: Select this option to sort and display the alerts based on their creation date.
  - **Updated**: Select this option to sort and display the alerts based on the date that they were updated on.
  - **Change sort order**: Select this option to display the alerts in an ascending or descending order.
  - **Refresh**: Select this option to refresh the alerts display.

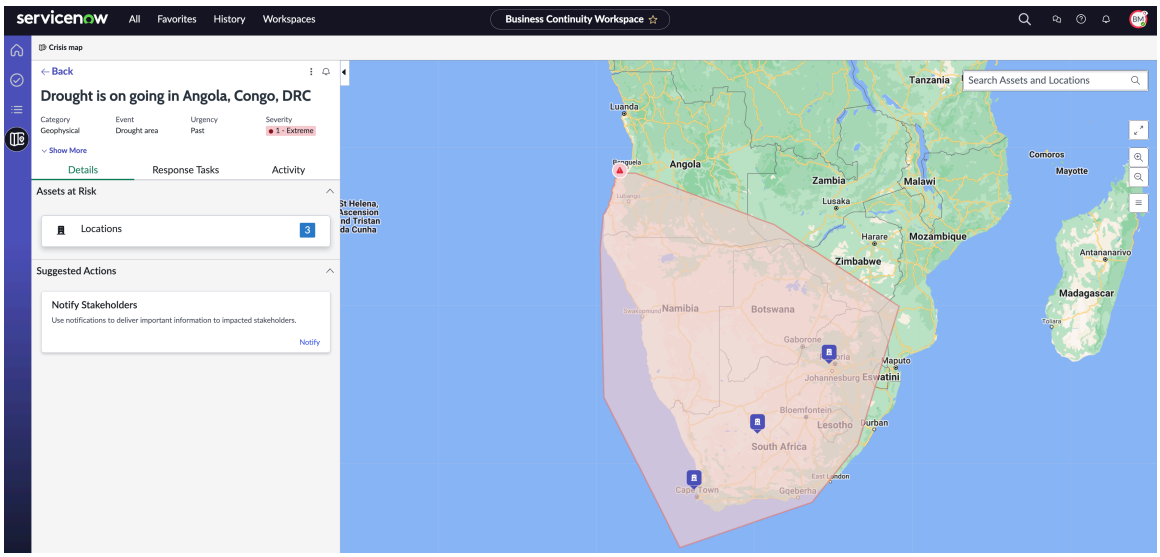
You can open or dismiss an alert in the alerts panel. You can also subscribe to an alert by selecting the bell icon as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## Alerts panel

When you select an alert in the **Alerts** panel, it launches a zoomed-in view with the alert details such as category, event, and so on as shown in the following example.




You can view the following details of a single alert in the Alerts panel:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

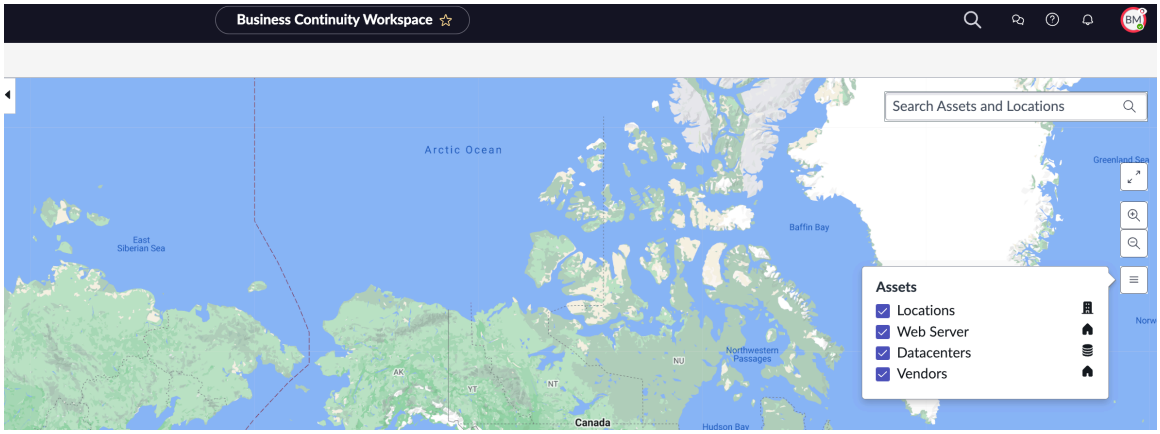
**Information in the Alerts panel**

| Field | Description |
|---|---|
| Title of the alert | Title of the alert such as Drought is on going in Angola, Congo, DRC. |
| Category | Category of the alert such as Geophysical. |
| Event | Event of the alert such as Drought area. |
| Urgency | Urgency of the alert such as Past. |
| Severity | Severity of the alert such as Extreme. |
| Certainty | Certainty of the alert such as Unknown. |
| Source | Source of the alert such as GDAC. |
| Latitude | Latitude of the alert such as -14.0701845. |
| Longitude | Longitude of the alert such as 13.0958574. |
| Web URL | Web URL of the alert such as Web https://www.gdacs.org/report.aspx?eventtype=DR&eventid=1014416. |
| Description | Description of the alert such as The Drought alert level is Red. |
| Details tab | |
| Assets at risk | Number of assets that are at risk as per locations. You can select the locations to view details such as Name, Contact, Phone, City, Latitude, Longitude, Updated, and so on. The Map view in the right panel shows the zoomed-in location and highlighted area of the alert. |
| Response tasks | Response tasks that are associated with the alert. |
| Activity | Activity related to the alert. It displays the Activity panel and the Compose section where you can add your notes. |
| Suggested actions | Suggested actions for the alert. For example, Notify Stakeholders: Use notifications to deliver important information to impacted stakeholders. |
| Back | Option to navigate to the Alerts panel view. |

## Map view in Crisis map

After you have set up Google maps, you can view the locations of the alerts in the Map view as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




You can view the following details in the Map view:

### Details in the Map view

| Icons | Description |
|---|---|
| **Search Assets and Locations** search bar | Search bar in the Map view. You can enter a location or a datacenter that is impacted by an alert. When you search for a location, a mixed list of your company results with the display value of the records along with their icons, and the Google map pin icons is displayed. |
| zoom-in ( ) and zoom-out ( ) | Zoom control buttons to change the zoom level of the map and view specific areas. |
| Layers icon ( | Layers icon to select and display the assets such as asset locations, datacenters, or core companies on the map.<br><br>The layers on the map are displayed as pins on a Google map and they are configurable. All the layer details such as the asset locations, assets, datacenters, and core companies are displayed on the map by their configured icons.<br><br>Use the Layers icon to view only the selected or all assets that can be toggled on and off on the map. As a crisis manager, when viewing the active alerts you can make an informed decision by concentrating on a single asset that can be critical at that moment from the rest. The following assets are displayed:<br>• Locations<br>• Web Server<br>• Datacenters<br>• Vendors |
| Reset icon ( | Reset icon to clear the map of all the search results. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Business impact analysis

Business impact analysis is a structured process where you assess the impact categories and dependencies and predict the consequences of a disruption on a business process or business function.

## An integral component of your business continuity plan

A business impact analysis is an integral component of the business continuity plan for an organization. It includes information on the important information systems and a planning component that includes the strategies for minimizing your risks.

Business managers have to make challenging decisions that can contribute to overall business growth. Sometimes, an unforeseen event or a disruption can cause disruptive effects. Performing a business impact analysis helps your business to mitigate these concerns. By evaluating the potential impact of an event or a decision, your business can predict future consequences and recover from setbacks successfully.

For information on the use cases for business impact analysis, see Use cases for business impact analysis.

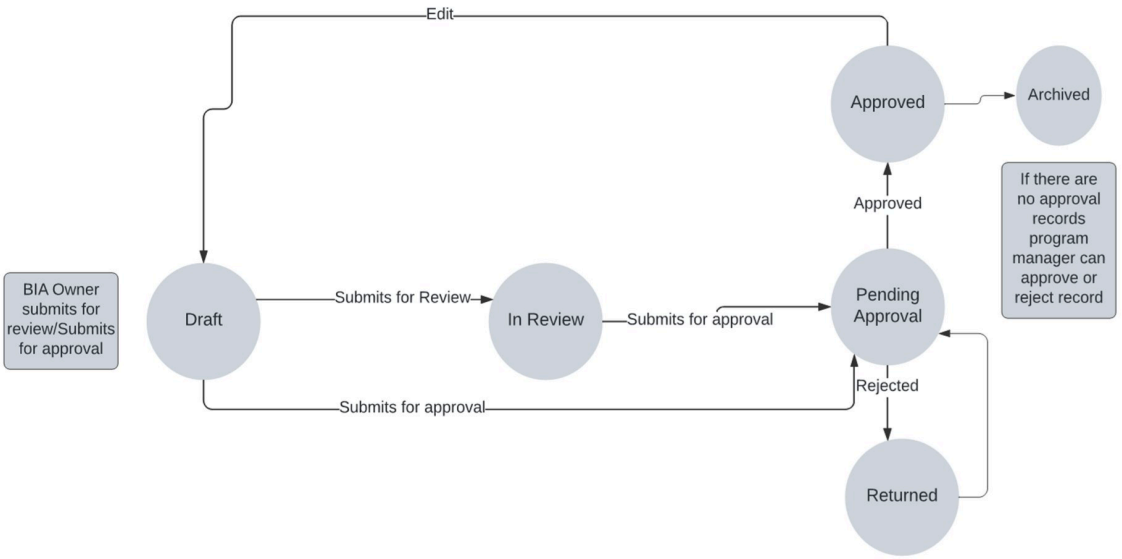
## Steps involved in creating a business impact analysis

Typically, the following steps involved in creating a business impact analysis:

- The business impact analysis owner creates a business impact analysis either from the Home page or the business impact analysis record page in the List view of the BCM UIB Workspace.
- The BIA owner adds additional details for the business impact analysis on the **Details** tab.
- Different users of the BCM application respond to the assessment questionnaire for the business impact analysis on the **Assessment** tab.
- Based on the responses received, the BCM application calculates the recovery time objective (RTO), recovery point objective (RPO), and dependencies for the business impact analysis.
- The business impact analysis owner reviews the information and submits the analysis for a review and approval to the business manager for services or IT manager for applications respectively.
- The business manager, IT manager, or BCM lead review the details of the business impact analysis and approve or reject it.
- An approved business impact analysis is moved to **Approved** and later, it is moved to the **Archived** state.
- The business impact analysis owner can generate the PDF of the analysis and save a copy for reference.

A typical business impact analysis workflow is shown in the following example:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



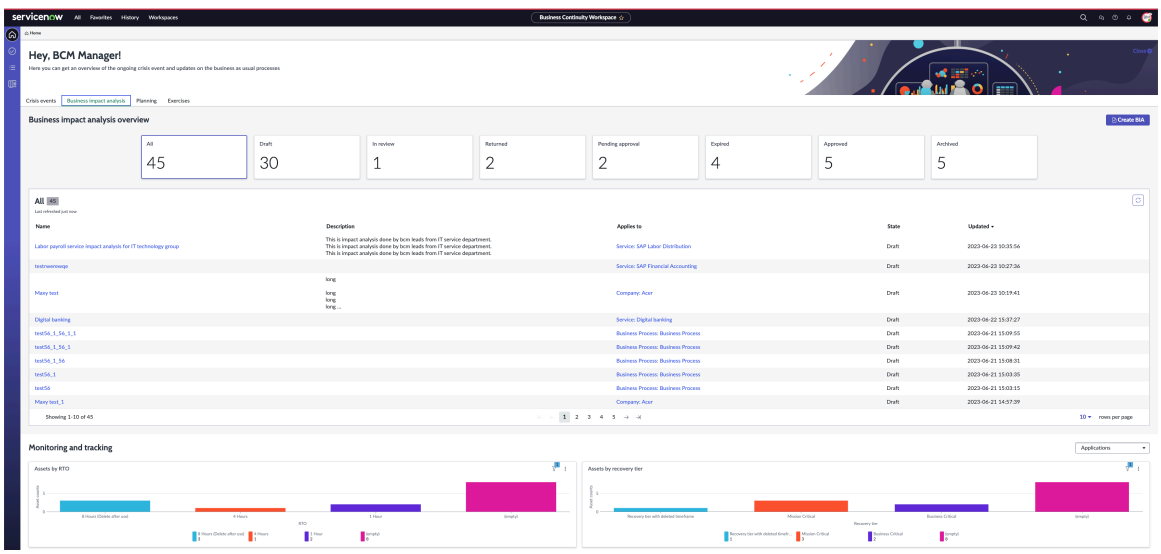

## Setup tasks for the business impact analysis administrator

If you are the business impact analysis administrator, you can view Setup for a business impact analysis for information on the setup tasks.

## Creating a business impact analysis in Business Continuity Workspace

if you are the business impact analysis owner, you can create a business impact analysis in Business Continuity Workspace by using one of the following options:

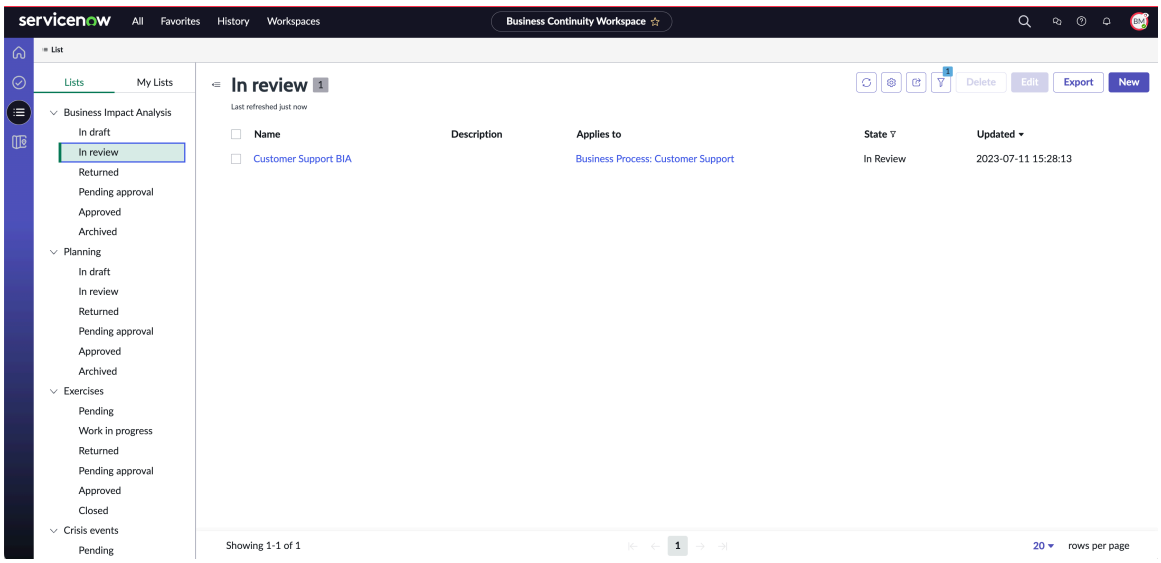
- You can navigate to the **Business impact analysis** tab in the Home page and select **Create BIA** as shown in the following example.




For the description of the cards and action buttons in the **Business impact analysis** tab of the Home page, see Home page view.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You can also navigate to the List view and select **New** in the Business Impact Analysis records as shown in the following example.




To create a business impact analysis in Business Continuity Workspace, see Create a business impact analysis. For information on managing the tasks that are related to a business impact analysis, see Structured workflows for Business Impact Analysis in BCM UIB Workspace.

### Use cases for business impact analysis

You can use the Business Continuity Management application to assess the impact of a downtime on your business services or processes and technical entities such as datacenters or applications. For creating a business impact analysis for your organization, you can refer to the common use cases that are used for managing the business continuity tasks.

**Note:** Every customer's environment is different. These use case scenarios only show generic implementations for the stated use cases. Your actual implementation may be different.

## Importance of performing the impact analysis

Performing the impact analysis is an important step in managing your business continuity tasks. It offers the following benefits:

- Prevents and minimizes unintended disruptions to your normal business functions.
- Helps you identify the critical business processes for your organization and develop strategies to prevent future issues.
- Assists in planning for the protection of your financial and technical assets.
- Offers guidance and support about the areas of improvement in future.

## Categories of impact analysis

You can broadly classify the impact analysis in the following categories:

Business impact analysis

If you are a business user who mainly manages the business services or processes, you want to determine the impact of a downtime on your services and processes. Performing a process-related business impact analysis can help your business to achieve the following objectives:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Prepare for the changes to a process or procedure.
- Identify the issues that are associated with a process.
- Mitigate for the risks that you may face due to an unexpected event.

Technical impact analysis

If you are an application user or the IT manager who mainly manages a datacenter or IT systems, you want to determine the impact of a downtime on your data and applications. Performing a technical impact analysis can help you to analyze the impact of technical changes in the deployed product or application. It gives the information about the areas of the information system that may be affected due to a change in the particular section or features of an application.

## Goal and method for creating the business impact analysis

Business impact analysis is typically performed by the business users to analyze a business service or business process. For example, if you are a financial analyst, you can perform the business impact analysis to estimate the impact of the downtime of a business process or service.

Goal

The goals of performing a business impact analysis are to determine the following information:

- Determine the criticality of the process.
- Determine the time that a business can survive without the business service or process.

Method to perform the business impact analysis

As a business user, you want to analyze the business service or process by estimating responses to few of the following assessment questions:

- What are the Impact categories or factors that affect the business service or process?
- What is the impact of the downtime of the business process or service?
- How many customers are affected?
- What is the revenue impact of the downtime for the organization?
- Are there additional penalties that the organization may incur?
- Is there a reputational damage for the organization?
- What is the additional cost to repair the damage such as media coverage of the estimated downtime?
- What supporting systems are required on a normal day so that the business processes run efficiently?

As the BCM lead or manager, when you respond to these assessment questions, it helps you to define the goals of creating a business impact analysis.

## Goal and method for creating the technical impact analysis

Technical impact analysis is typically performed by the IT owners to analyze the applications or systems that house the data. For example, if you are an IT owner of a financial organization, you can perform the technical impact analysis to determine the criticality and timelines for the applications and frequency to back up the data.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Goal

The goals of performing a technical impact analysis are to determine the following information:

- Criticality of the application.
- Timeline that the organization can survive for without the application.
- Frequency to back up the data

Method to perform the technical impact analysis

As a business user, you can perform the business impact analysis by estimating the responses to the following sample assessment questions:

- What is the impact on the business if the application is non-functional?
- How many employees are impacted?
- Is the application external facing?
- How many customers are impacted, if the application is external facing?
- What kind of data does the application process?
- How frequently does the data change?

As the business user, when you respond to these assessment questions, it helps you to define the goals of the technical impact analysis.

## Using the business impact analysis workflow

If you are a user of the BCM application, you can use the business impact analysis workflow to perform the business impact analysis.

The following sample use cases are considered for creating a business impact analysis with BCM:

- Assess the recovery tier for the business processes or applications that are based on the pre-defined templates.
- Identify the recovery point objective.
- Identify the recovery time objective.
- Identify the dependencies such as vendors, applications, facilities, and other foundational elements.

As a pre-requisite to the business impact analysis workflow, the BCM administrator of your organization sets up the BIA template in the BCM application. The template offers a survey-type user experience in the form of an assessment questionnaire.

If you are the BCM administrator, you can set up the questions that are relevant to your organization and scenario in the BIA template. For more information on setting up the BIA template with the BCM administrator role, see Configure a business impact analysis (BIA) template.

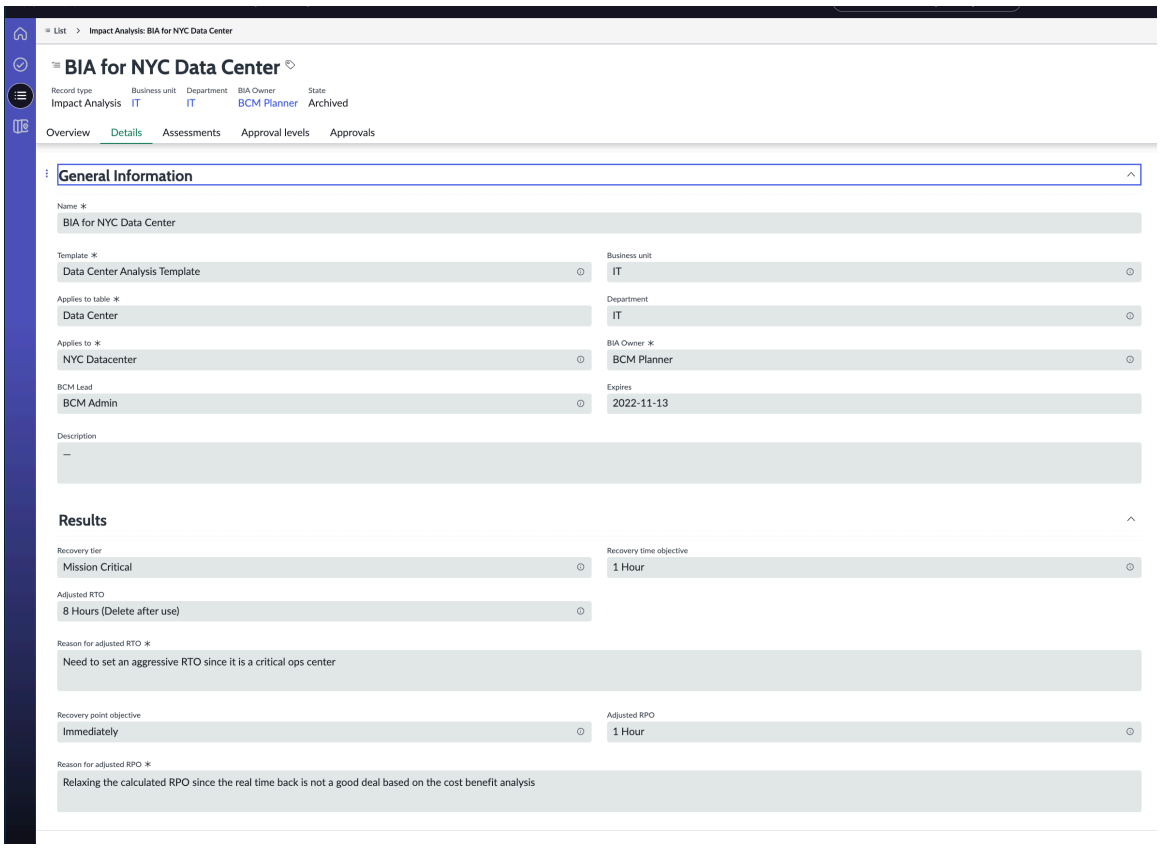
If you are the BCM lead or BCM program manager, you can respond to the assessment questionnaire on the **Assessments** tab of the business impact analysis record. If you mainly use the business services and processes, your answers serve as key data points for the recovery time objective assessment and dependency assessment. Based on your responses, the criticality of the business process or service and recommended timelines are determined.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you are the BCM lead or BCM program manager who handles the IT systems, data, and applications, your answers serve as key data points for the recovery point objective assessment. Based on the responses received to the questionnaire, the application calculates the criticality of the business process or service and the recommended timelines.

## Outcome of the impact analysis in BCM

After receiving responses to the questionnaire, the BCM application calculates the results of the business impact analysis. The results are displayed in the **Results** section on the **Details** tab in the business impact analysis record as shown in the following example.




The BCM application displays the following key results in the business impact analysis record:

Recovery tier

The BCM application determines the criticality of the process. It is known as the recovery tier. For example, a recover tier can be non-essential or critical for your business.

Recovery time objective

The BCM application helps you to determine the time that the organization can survive without the business process that is the recovery time objective (RTO).

Adjusted RTO

The business impact analysis owner can adjust the recovery time objective value for practical reasons. The adjusted value is displayed in the **Adjusted RTO** field in the **Results** section. If you are the business impact analysis owner and you have adjusted the RTO value with a reason during the assessment, the reason for the adjustment is displayed in the **Reason for adjusted RTO** field.

Dependencies

The BCM application helps you to determine the supporting systems or dependencies that are required on a normal day so that the business processes

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

run efficiently. For example, you can have the following dependencies for your business:

- People
- Facility
- Application
- Vendors

For more information on the recovery time objective, recovery point objective, and recovery tiers, see Recovery time objective, Recovery point objective, and Recovery tiers.

### Business impact analysis (BIA) templates

The Business Continuity Management application provides pre-configured business impact analysis (BIA) templates for creating a business impact analysis. If you are the BCM or BIA administrator, you can use the **BIA Templates** module in the Business Continuity Management application. You can then select the type of the template, elements, impact categories, and so on, for the business impact analysis.

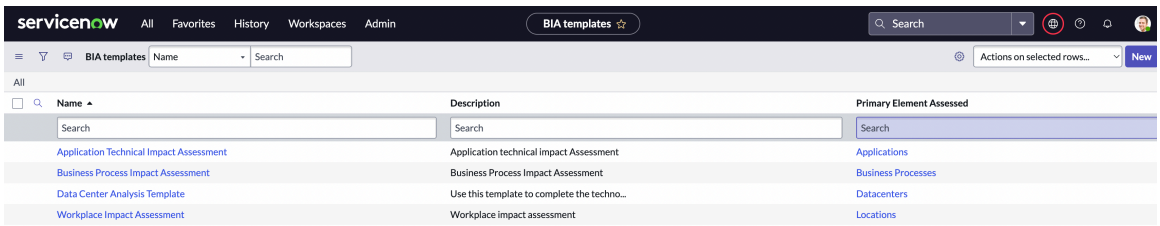
## Advantages of using a BIA template

The BIA templates store information such as the impact categories and dependency groups that a business process depends on. Using a BIA template offers the following advantages:

- Simplifies the process of creating a business impact analysis.
- Saves time and resources by pre-populating the templates.
- Helps you to define the primary object type that you can use the BIA template for. For example, you can use the Application technical impact analysis template to perform a technical impact analysis of an IT application.
- Populates the dependency groups automatically in the BIA.
- Helps you to select the impact categories that are relevant to your organization.

## BIA templates in BCM

If you have the sn_bcm.admin role, you can view the BIA templates that are installed with demo data when you install the application or configure a BIA template in the **BIA Templates** module. The following example shows the BIA templates that are installed with demo data in the Business Continuity Management application.




## BIA template configuration

With the sn_bcm.admin role, you can configure the following details in the BIA template:

Name and Description

Use the **Name** and **Description** fields to search for the name and select an appropriate template for your business impact analysis.

Primary Element Assessed

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Select the type of the elements that you plan to assess such as Business processes or CI service.

Impact Categories

Assess specific impact categories during the business impact analysis. For example, you plan to assess the financial impact and legal impact of a downtime.

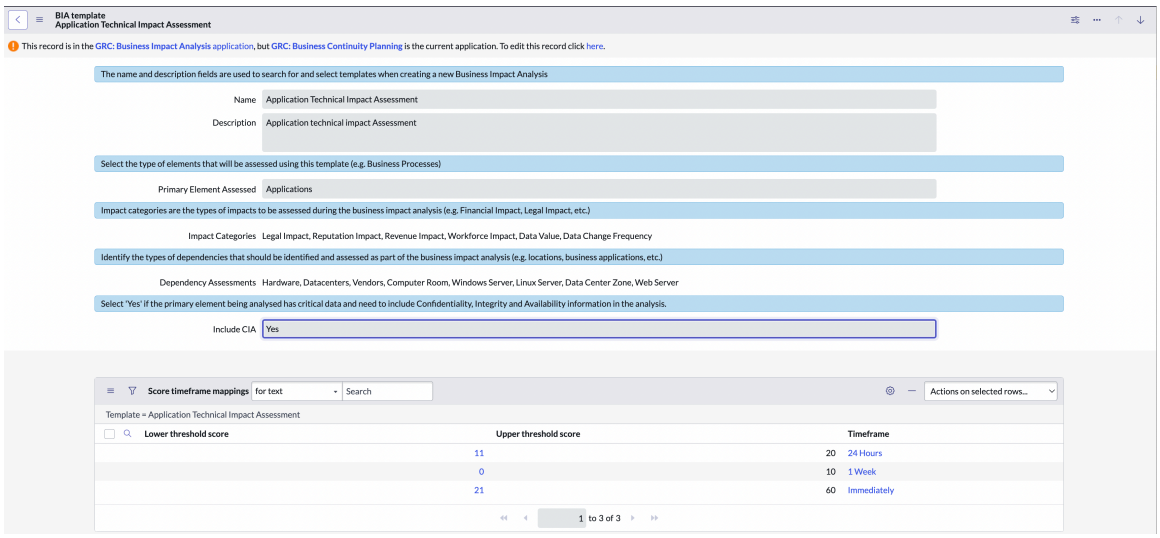
Dependency Assessments

Identify the dependencies for your business impact analysis.

Include CIA

Include CIA (Confidentiality, Integrity, Availability) information in your business impact analysis if the primary element being analyzed has critical data.

The following example shows the sample configuration of a BIA template in an instance.




## Configuring a BIA template

For more information on how to configure a BIA template with the sn_bcm.admin role, see Configure a business impact analysis (BIA) template.

### Element definitions and variables

An element definition is a configuration item that is assessed in the business impact analysis. The element definitions are also recovered in the business continuity plan. If you have the administrator role, you can set up an element variable that is required for a particular dependency of an element.

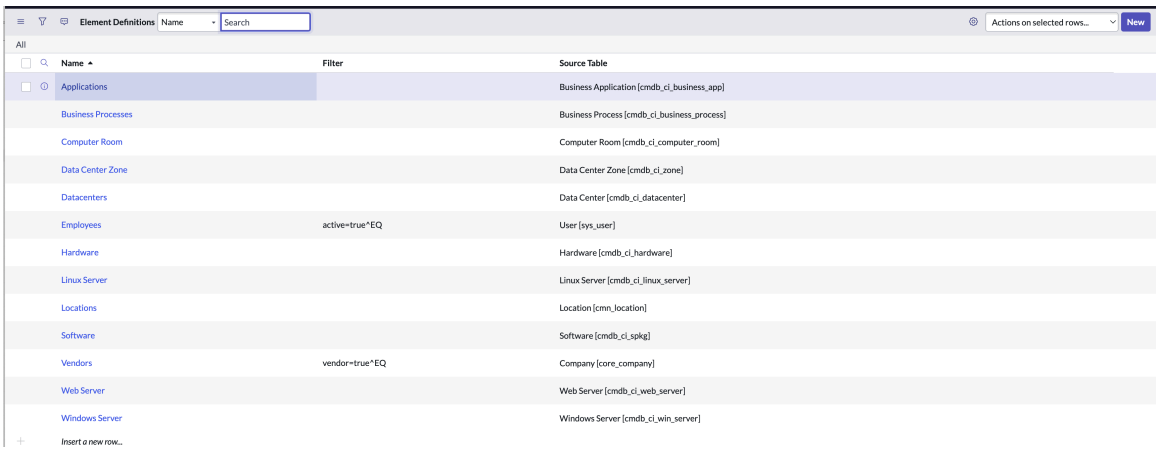
The BCM administrator can configure the element definitions in the Business Continuity Management application. Typically, the following element definitions are defined in the Business Continuity Management application:

- Applications
- Business Processes
- Computer Room
- Datacenter Zone
- Datacenters
- Employees

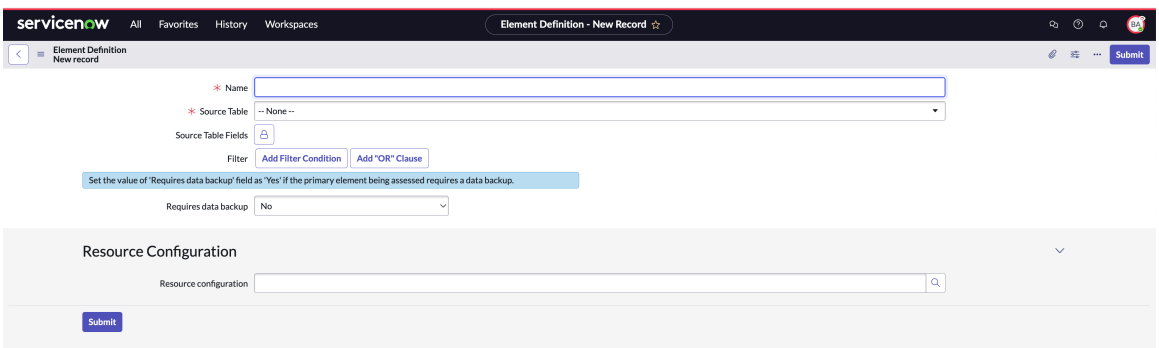
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Linux Server
- Locations
- Software
- Vendors
- Web Server
- Windows Server

The following example shows the element definitions in an instance.




The following example shows the configuration of an element definition by the Business Continuity Management administrator.



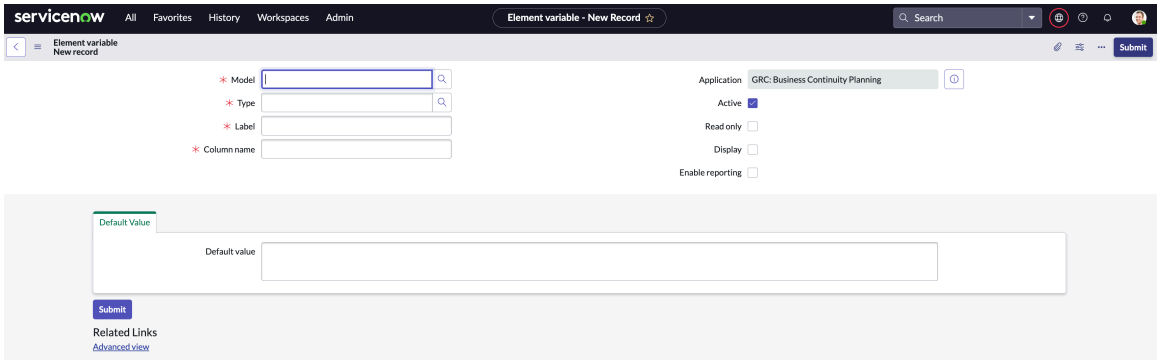

## Configuration of an element definition

For more information on configuring an element definition with the BCM administrator role, see Configure an element definition for the business impact analysis.

## Configuration of an element variable

As a functional system administrator, you can set up an element variable that is required for a particular dependency of an element. The following example shows an administrator's view of the element variable record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

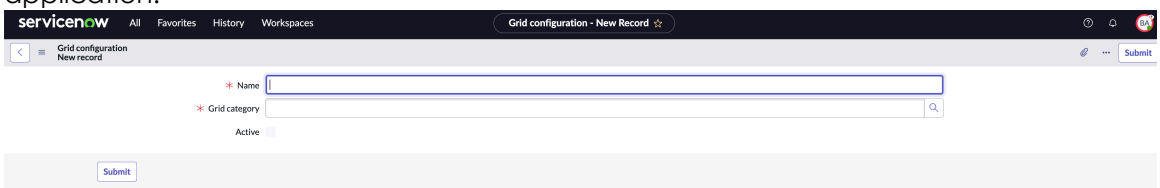



For more information on how to configure an element variable in the Business Continuity Management application with an administrator role, see Configure an element variable for an element definition.

### Grid configurations and categories

You can set up the grid configuration to render the BIA dependency assessment grid with configured columns. You can define the grid category such as Dependency Assessment for which the grid configuration is applicable.

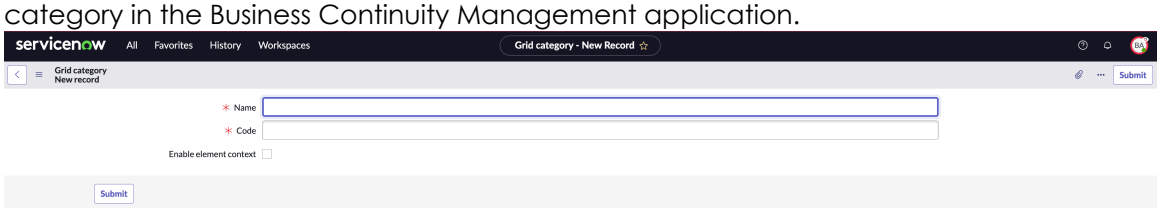
The following example shows the grid configuration in the Business Continuity Management application.




**Note:** Grid configuration is used in BCM classic Workspace only. Starting with the Utah release, the BCM classic Workspace is being prepared for future deprecation.

For more information on how to configure the grid in the Business Continuity Management application, see .

The following example shows the configuration of a grid category in the Business Continuity Management application.




**Note:** Grid categories are used in BCM classic Workspace only. Starting with the Utah release, the BCM classic Workspace is being prepared for future deprecation.

## Business continuity planning

Business continuity planning helps you enact and mitigate risk at the time of an event. You can address and plan on the primary scope of the activities, documentation, loss scenarios, recovery teams, approvals, and so on. You can then configure a structured workflow of your business continuity planning tasks in BCM UIB Workspace.

When you create a comprehensive business continuity plan for different possible disruptive scenarios, your organization is equipped to face a crisis or any adverse situation.

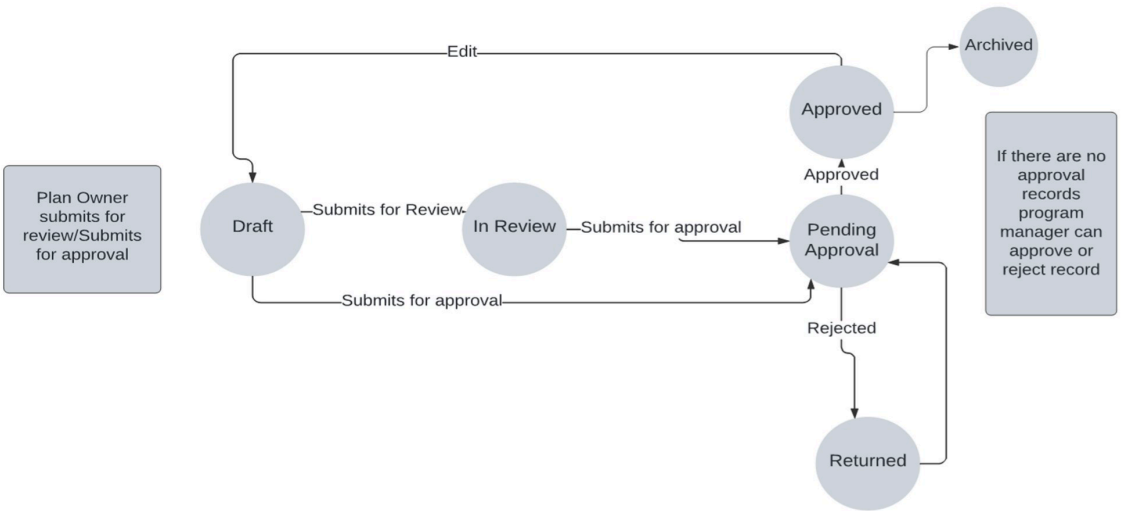
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Steps involved in creating a business continuity plan

Typically, the following steps involved in creating a business continuity plan:

- The BCM program manager or planner creates a business continuity plan either from the Home page or the Planning record page in the List view of the BCM UIB Workspace.
- The BCM program manager or planner adds additional details for the business continuity plan such as its scope, documentation section, recovery teams, related plans, and so on.
- The business impact analysis owner reviews the information and submits the analysis for a review and approval to the business manager for services or IT manager for applications respectively.
- The business manager, IT manager, or BCM lead review the details of the business continuity plan and approve it.
- The approved business continuity plan is moved to **Approved** and later, it is moved to the **Archived** state.
- The business continuity plan owner can generate the PDF of the plan and save a copy for reference.

A typical business continuity plan workflow is shown in the following example:




## Setup tasks for business continuity planning

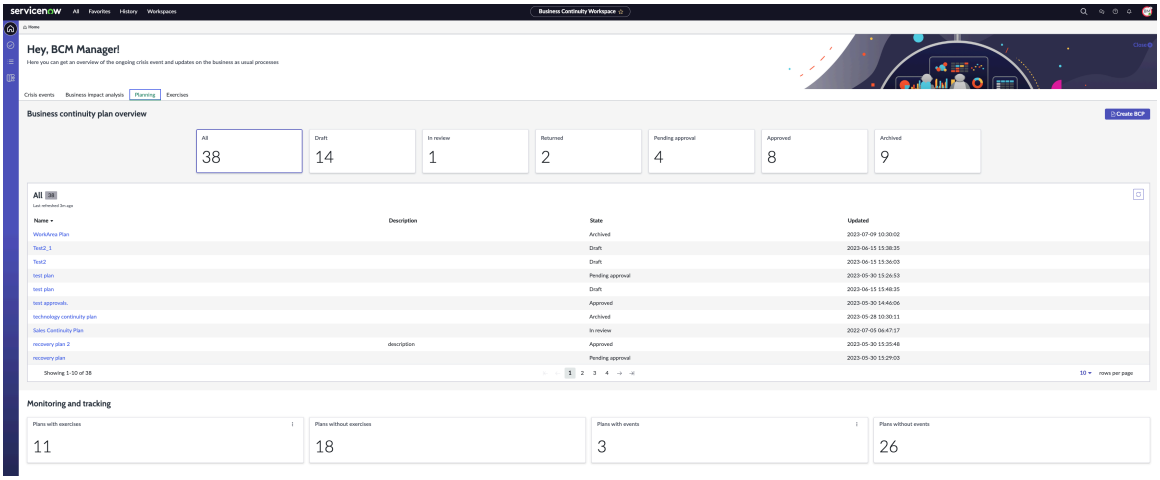
If you are the BCP administrator, you can view Setup for a business continuity plan for information on the BCP setup tasks.

## Creating a business continuity plan in Business Continuity Workspace

if you are the business continuity plan owner, you can create a business continuity plan in Business Continuity Workspace by using one of the following options:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You can navigate to the **Planning** tab in the Home page and select **Create BCP** as shown in the following example.




  For the description of the cards and action buttons in the **Planning** tab of the Home page, see Home page view.

- You can also navigate to the List view and select **New** in the Planning records.

To create a business continuity plan in Business Continuity Workspace, see Create a business continuity plan. For information on managing tasks related to a business continuity plan, see Structured workflows for Business Continuity Planning in BCM UIB Workspace.

### Assets and plans related to a business continuity plan

You can identify the assets and plans related to a business continuity plan. You can then recover the assets in your planning stage. Reuse the configuration item relationship data that flow from CMDB to business impact analysis (BIA) during dependency assessment to identify the assets in your plan.

## Related Assets

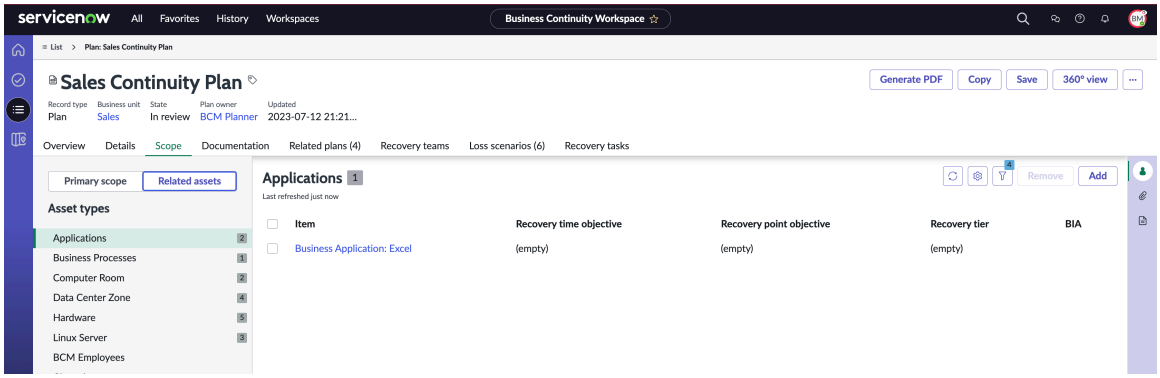
If you have added a business process or a location as an item in the **Primary scope** panel of the record, and if the scoped item is related to the business impact analysis, then all the related assets of the business impact analysis are listed in the **Related assets** panel in the record.

In other words, the CMDB configuration item added as a dependency in the business impact analysis is pulled into the plan as a related asset. The source of these related assets is displayed as the business impact analysis.

When you create a plan, you also select a primary element that the plan covers. Based on the scope that you selected in the business continuity plan or the primary element of the plan, the application adds the related assets and related plans during the planning phase. These items could be business processes, critical business applications, datacenters, or resources working from a location. All these dependencies if stored in the business impact analysis are copied over to the plan in the **Related assets** panel in addition to other dependencies that are added while creating the business impact analysis.

The following example shows the primary scope and related assets for a business continuity plan.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## Related plans

After the assets are copied over to the plan, if there are plans attached to any of the related assets, then these plans are automatically pulled and listed on the **Related Plans** tab. Assets in the plan are the entities that are to be recovered by the plan during the event. When the related plans are pulled into the planning phase, you can also create the recovery tasks. As a planner, you can set a sequence to the execution of the recovery tasks of the main plan and its dependent subplans.

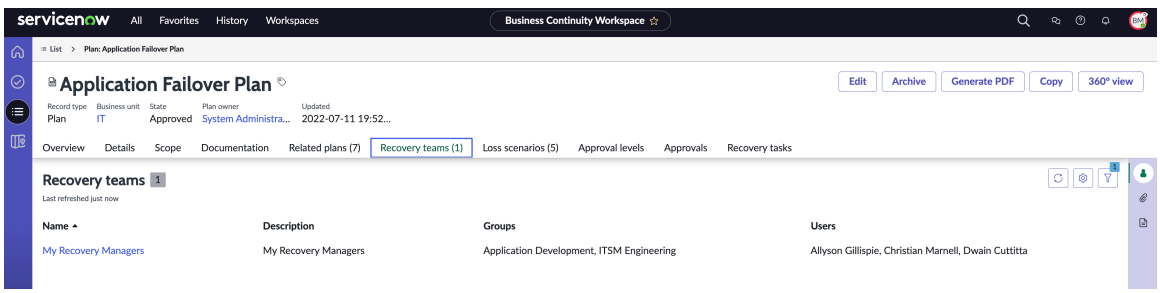
### Recovery teams, loss scenarios, and recovery tasks

Business continuity planning workspace guides you to complete your business continuity plan. You can create a recovery team, define roles for the users, and direct the team to execute the plan. When you create a continuity plan for a department or a business unit, it is necessary to identify the loss scenarios to the business continuity plan.

## Recovery teams

You can create a recovery team by entering the name and description for a recovery team or update an existing recovery team. You can select one or more users and groups from the respective lists.

The description for the recovery team also indicates the responsibilities of the users and groups who are assigned to the recovery team. You can also create a recovery team and add the user and group assignment later as shown in the following example.



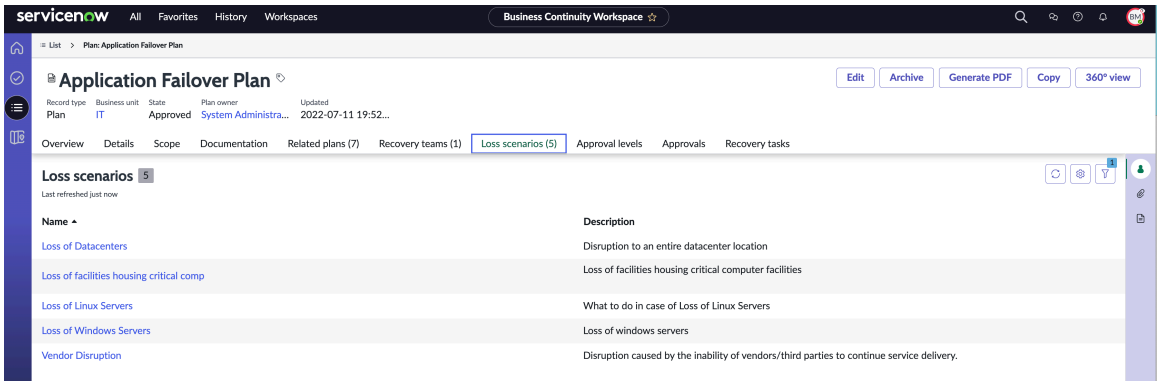

## Loss scenarios

Identifying a loss scenario helps your business to be prepared for future disruptive events and continue with your business functions as usual.

If you have the BCM administrator role, you create a business continuity plan by using the plan template. The loss scenarios that are identified in the plan template automatically get associated to the plan that you have created.

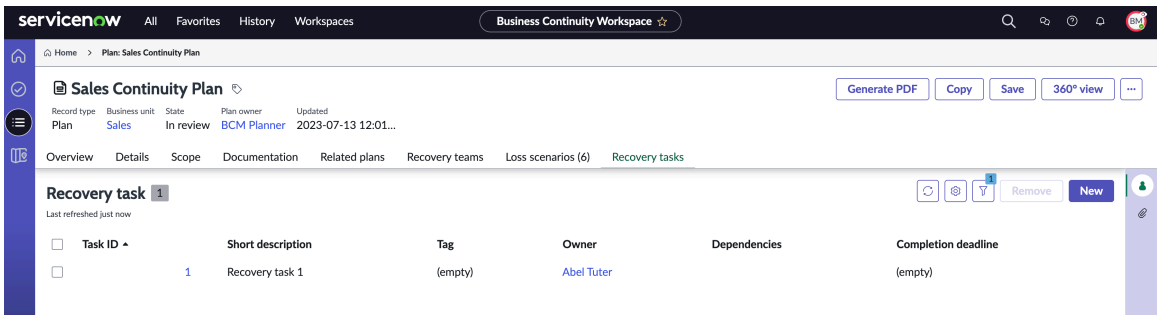
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Your plan has a basic set of loss scenarios attached to it. You can then add additional loss scenarios to the plan as per your requirement in the BCM UIB Workspace as shown in the following example.




## Recovery tasks

You can assign the recovery task to a group by identifying an owner to execute the processes and procedures of a recovery. The recovery task contains the details of the item to be recovered and the time by which it should be accomplished as shown in the following example.




## Exercises

Exercises are used to provide continuous testing and improving of continuity plans. You can use the exercises to finalize your business continuity plan and improve its effectiveness and usability in an actual crisis event. You can manage your exercises in BCM UIB Workspace.

## Steps involved in creating an exercise

Typically, the following steps are involved in creating an exercise:

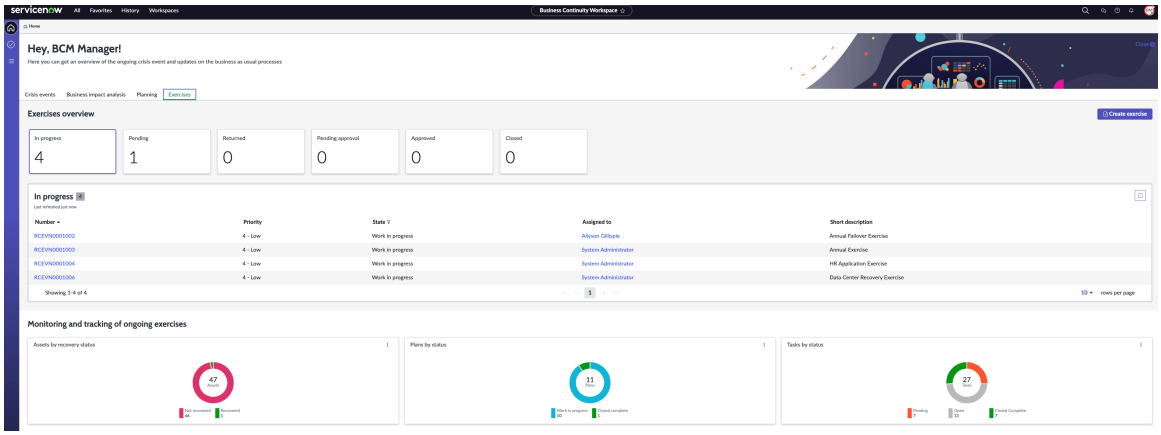
- The BCM program manager creates an exercise either from the Home page or the Exercises record page in the List view of the BCM UIB Workspace.
- The BCM program manager adds additional details for the exercise such as an asset, plan, and event task.
- The BCM program manager submits the event task related to the exercise for an approval.
- The assigned BCM program manager reviews the details on the event task and approves the exercise.
- The exercise is moved to the **Approved** state. An approved exercise is moved to the **Archived** state later.
- The BCM program manager can generate the PDF of the details and save a copy for reference.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Creating an exercise in Business Continuity Workspace

If you are the BCM program manager, you can create an exercise in Business Continuity Workspace by using one of the following options:

- You can navigate to the **Exercises** tab in the Home page and select **Create exercise** as shown in the following example.




  For the description of the cards and action buttons in the **Exercises** tab of the Home page, see Home page view.

- You can also navigate to the List view and select **New** in the Exercises records.

To create an exercise in Business Continuity Workspace, see Structured workflows for Exercise Management in BCM UIB Workspace.

## Crisis events

Managing a crisis event in BCM UIB Workspace helps you to minimize the downtime of critical business functions and processes across your organization. It is also used to minimize the financial, reputation, legal, and regulatory impact during a crisis event.

### Steps involved in creating a crisis event

Typically, the following steps are involved in creating a crisis event:

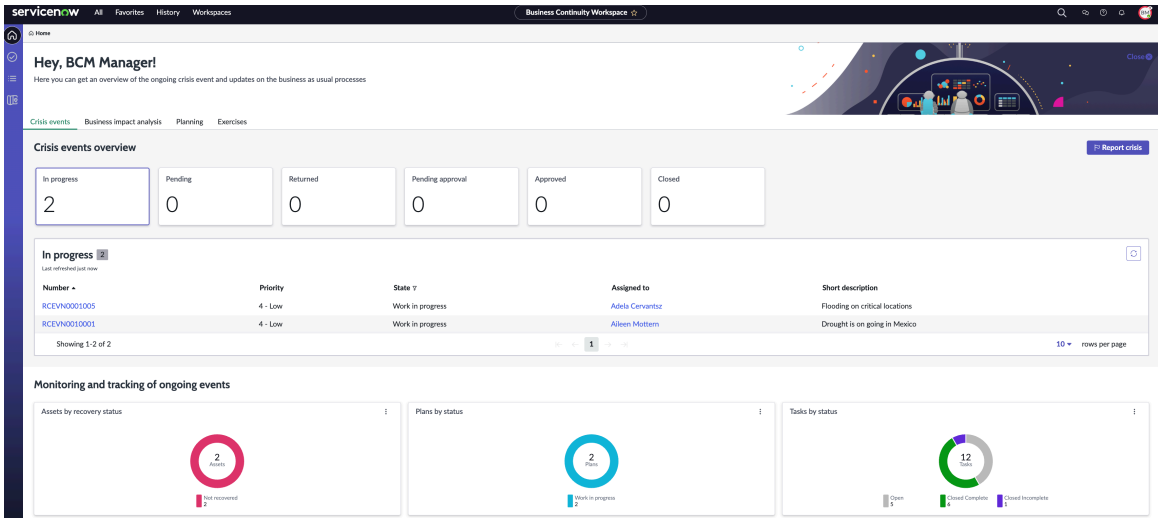
- The BCM program manager creates a crisis event either from the Home page or the Crisis events record page in the List view of the BCM UIB Workspace.
- The BCM program manager adds additional details for the crisis event such as an asset, plan, and event task.
- The BCM program manager submits the event task related to the exercise event for an approval.
- The assigned BCM program manager reviews the details on the event task and approves the event.
- The crisis event is moved to the **Approved** state. An approved crisis event is moved to the **Archived** state later.
- The BCM program manager can generate the PDF of the details and save a copy for reference.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Creating a crisis event in Business Continuity Workspace

if you are the BCM program manager, you can create a crisis event in Business Continuity Workspace by using one of the following options:

- You can navigate to the **Crisis events** tab in the Home page and select **Report crisis** as shown in the following example.




  For the description of the cards and action buttons in the **Crisis events** tab of the Home page, see Home page view.

- You can also navigate to the List view and select **New** in the Crisis events records.

To create a crisis event in Business Continuity Workspace, see Structured workflows for Crisis Management in BCM UIB Workspace.

## Crisis map interface

You can integrate Crisis map with the BCM application and initiate the response workflows for crisis management. After installing the Crisis map application, you can view the **Threat and Alert Data Feeds** module in your BCM application instance.

## Feeds, alerts, and events in BCM

When you integrate the Crisis map application with the BCM application, you can view and analyze the feeds, alerts, and events from different locations in the Crisis map view.

Feed

A feed is news content updated frequently and provided on a worldwide website. You can subscribe to a news feed by manually entering the URL of the feed channel in the **Web** field of the Feed form.

Alert

An alert is a notification that reports an incident happened at a particular place and time. First, an incident, or an event reportedly happens. Then, the alert triggers a notification that reports or notifies the incident to the concerned people to take an action.

Event

Based on the severity of the alerts, you can take actions such as notifying the stakeholders of the incident or declaring a crisis event. An event can become a crisis event if it disrupts the business operations. For information on the crisis

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

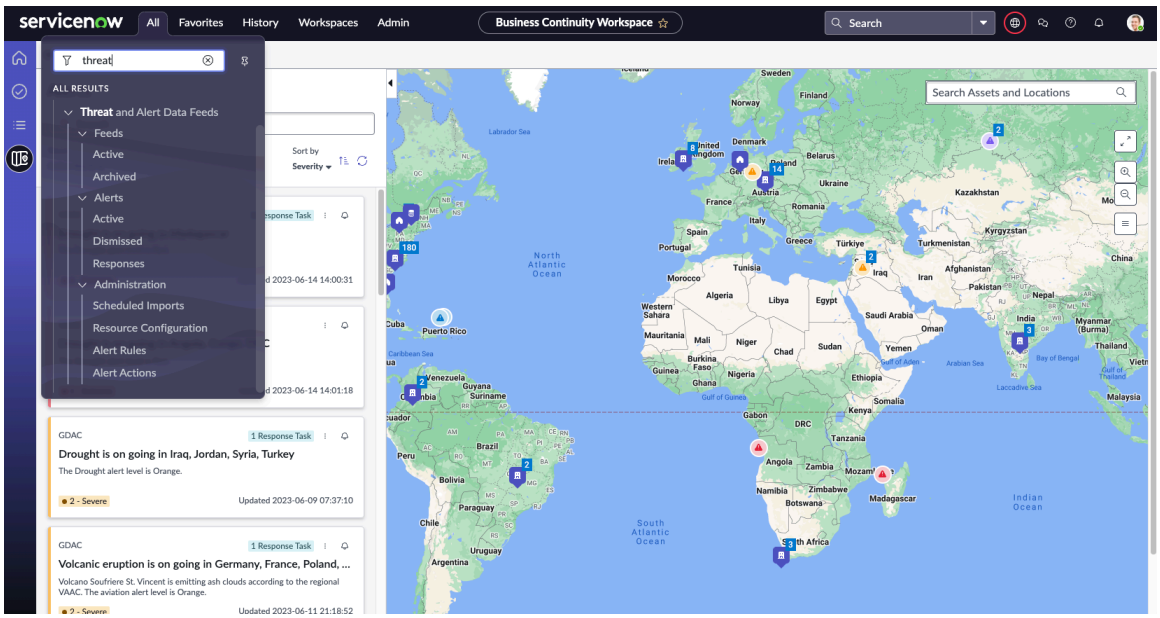
events, see Crisis map view. You can then activate the business continuity plans for the locations that are impacted by the event.

## Threat and Alert Data Feeds module in BCM

The **Threat and Alert Data Feeds** module in BCM displays the following information:

- **Feeds**
- **Alerts**
- **Administration**

The **Threat and Alert Data Feeds** module is shown in the following example.




## Feeds module in BCM

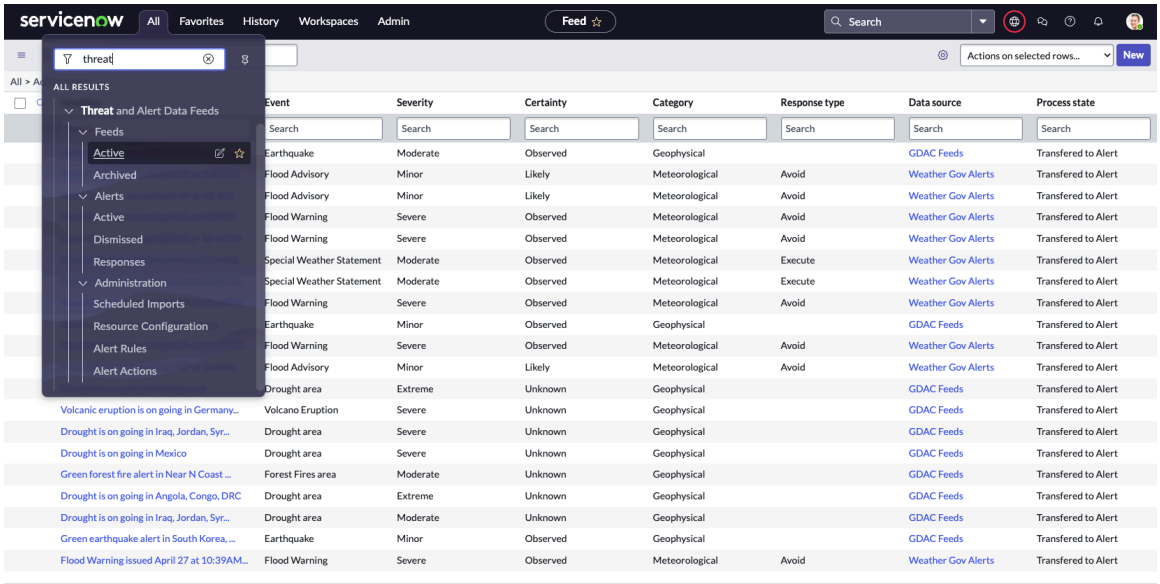
A threat feed is the data intelligence information of a potential or current threat that can pose a danger to an organization. It can disrupt the business routine or disable its business processes. The Crisis map application receives the feeds from third-party sources such as GDAC Feeds and Weather Gov Alerts.

The **Feeds** module in BCM displays the following types of feeds:

- **Active feeds**
- **Archived feeds**

A sample view of the active feeds is displayed in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




You can use the **Personalize List** icon to configure the list columns in the **Feeds** module. For example, you can display the following additional details on the alert:

- Headline
- Event
- Severity
- Certainty
- Category
- Response type
- Data source
- Process state

Threat feeds include information about real-time disruptive events as shown in the following sample list:

- Civil unrest or riots
- Flood advisory
- Flood warning
- Drought area
- Earthquake
- Hurricane
- Wildfire or red flag warnings
- War or military conflict
- Volcano eruption

## Alerts module in BCM

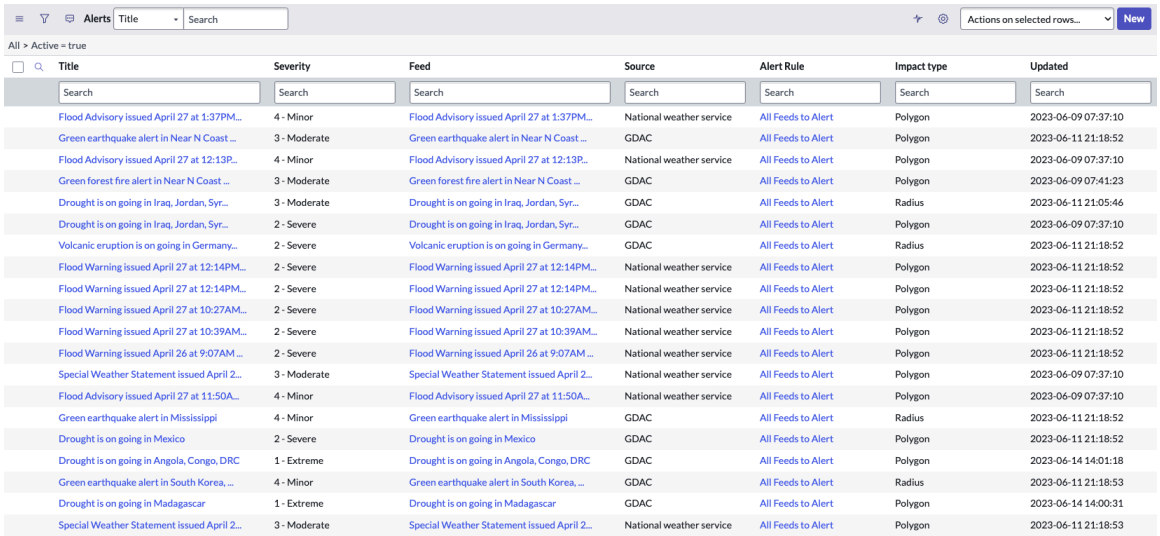
An alert is a notification that reports an incident happened at a particular place and time. First, an incident or an event reportedly happens. Then, the alert triggers a notification that reports or notifies the incident to the concerned people to take an action.

The **Alerts** module in BCM displays the following types of feeds:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Active alerts**
- **Dismissed alerts**
- **Alert responses**

A sample view of the active alerts is shown in the following example.




| Title | Severity | Feed | Source | Alert Rule | Impact type | Updated |
|---|---|---|---|---|---|---|
| Flood Advisory issued April 27 at 1:37PM... | 4 - Minor | Flood Advisory issued April 27 at 1:37PM... | National weather service | All Feeds to Alert | Polygon | 2023-06-09 07:37:10 |
| Green earthquake alert in Near N Coast ... | 3 - Moderate | Green earthquake alert in Near N Coast ... | GDAC | All Feeds to Alert | Polygon | 2023-06-11 21:18:52 |
| Flood Advisory issued April 27 at 12:13P... | 4 - Minor | Flood Advisory issued April 27 at 12:13P... | National weather service | All Feeds to Alert | Polygon | 2023-06-09 07:37:10 |
| Green forest fire alert in Near N Coast ... | 3 - Moderate | Green forest fire alert in Near N Coast ... | GDAC | All Feeds to Alert | Polygon | 2023-06-09 07:41:23 |
| Drought is on going in Iraq, Jordan, Syr... | 3 - Moderate | Drought is on going in Iraq, Jordan, Syr... | GDAC | All Feeds to Alert | Radius | 2023-06-11 21:05:46 |
| Drought is on going in Iraq, Jordan, Syr... | 2 - Severe | Drought is on going in Iraq, Jordan, Syr... | GDAC | All Feeds to Alert | Polygon | 2023-06-09 07:37:10 |
| Volcanic eruption is on going in Germany... | 2 - Severe | Volcanic eruption is on going in Germany... | GDAC | All Feeds to Alert | Radius | 2023-06-11 21:18:52 |
| Flood Warning issued April 27 at 12:14PM... | 2 - Severe | Flood Warning issued April 27 at 12:14PM... | National weather service | All Feeds to Alert | Polygon | 2023-06-11 21:18:52 |
| Flood Warning issued April 27 at 12:14PM... | 2 - Severe | Flood Warning issued April 27 at 12:14PM... | National weather service | All Feeds to Alert | Polygon | 2023-06-11 21:18:52 |
| Flood Warning issued April 27 at 10:27AM... | 2 - Severe | Flood Warning issued April 27 at 10:27AM... | National weather service | All Feeds to Alert | Polygon | 2023-06-11 21:18:52 |
| Flood Warning issued April 27 at 10:39AM... | 2 - Severe | Flood Warning issued April 27 at 10:39AM... | National weather service | All Feeds to Alert | Polygon | 2023-06-11 21:18:52 |
| Flood Warning issued April 26 at 9:07AM ... | 2 - Severe | Flood Warning issued April 26 at 9:07AM ... | National weather service | All Feeds to Alert | Polygon | 2023-06-11 21:18:52 |
| Special Weather Statement issued April 2... | 3 - Moderate | Special Weather Statement issued April 2... | National weather service | All Feeds to Alert | Polygon | 2023-06-09 07:37:10 |
| Flood Advisory issued April 27 at 11:50A... | 4 - Minor | Flood Advisory issued April 27 at 11:50A... | National weather service | All Feeds to Alert | Polygon | 2023-06-09 07:37:10 |
| Green earthquake alert in Mississippi | 4 - Minor | Green earthquake alert in Mississippi | GDAC | All Feeds to Alert | Radius | 2023-06-11 21:18:52 |
| Drought is on going in Mexico | 2 - Severe | Drought is on going in Mexico | GDAC | All Feeds to Alert | Polygon | 2023-06-11 21:18:52 |
| Drought is on going in Angola, Congo, DRC | 1 - Extreme | Drought is on going in Angola, Congo, DRC | GDAC | All Feeds to Alert | Polygon | 2023-06-14 14:01:18 |
| Green earthquake alert in South Korea, ... | 4 - Minor | Green earthquake alert in South Korea, ... | GDAC | All Feeds to Alert | Radius | 2023-06-11 21:18:53 |
| Drought is on going in Madagascar | 1 - Extreme | Drought is on going in Madagascar | GDAC | All Feeds to Alert | Polygon | 2023-06-14 14:00:31 |
| Special Weather Statement issued April 2... | 3 - Moderate | Special Weather Statement issued April 2... | National weather service | All Feeds to Alert | Polygon | 2023-06-11 21:18:53 |

You can use the **Personalize List** icon to configure the list columns in the **Alerts** module. For example, you can display the following details on the alert:

- Title
- Severity
- Feed
- Source
- Alert rule
- Impact type
- Updated

## Administrative tasks in the Threat and Alert Data Feeds module

If you have the BCM administrator role, see Setup for Crisis map for information on the setup tasks.

The **Administration** module in BCM displays the following types of feeds:

Scheduled imports

To manage your threat feed subscriptions that are sourced internally and externally, you must schedule a data import from the data source at defined intervals. For more information on scheduled imports, see Configure a Scheduled Data Imports record.

Resource configuration

To plot your organization's assets or resources on the Crisis map, you must configure the resources in the application. For more information on resource configuration, see Configure a Resource Configuration record for Crisis map.

Alert rules

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To display the feeds as alerts on the Crisis map, configure the alert rules. For more information on alert rules, see Configure an alert rule in Crisis map.

Alert actions

To act on a critical alert from the Crisis map dashboard, see Configure an alert action in Crisis map.

- For information on the administrative tasks for Crisis map, see Setup for Crisis map.
- To search for locations on the Crisis map, you must set the *sn_bcm_map.use_google_places_lib* system property. For more information, see Properties installed with Business Continuity Management.

### Crisis map

For information on managing the alerts in Crisis map, see Structured workflows for Crisis map in BCM UIB Workspace.

## Emergency notifications in Everbridge notifications system

You can integrate Crisis Management in the BCM application with Everbridge notifications system. You can then send an emergency notification to an individual or a group of people alerting them of an impending emergency. It provides a one-way notification and two-way communication through properly established delivery channels.

Crisis Management in Business Continuity Management application uses Everbridge to direct certain crisis response activities. This integration helps to send notifications about critical events to stakeholders and coordinates responses from them in an effective two-way delivery channel.

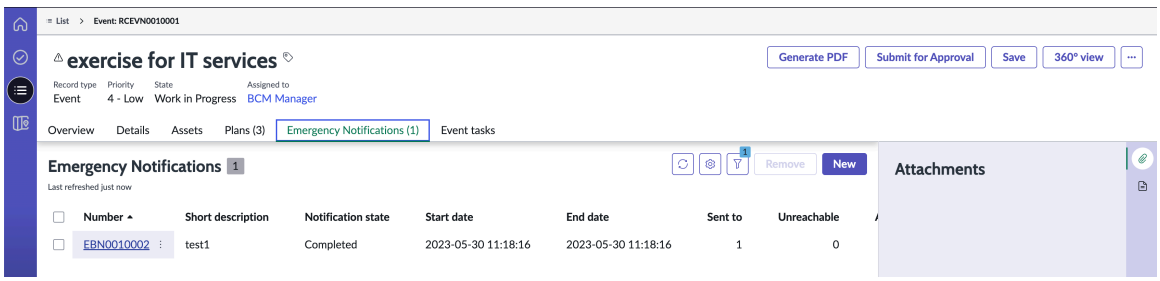
To send a notification, you need correct contacts, groups, and delivery channels. Delivery channels are created and stored in Everbridge and you have to import those delivery channels for your particular organization ID. These delivery channels are used for sending notifications and contact creation.

## Process for sending the emergency notifications

You can send an event notification that triggers a complete workflow of the activities from the **Draft** to the **Complete** state in Everbridge. You can monitor all activities from Business Continuity Workspace.

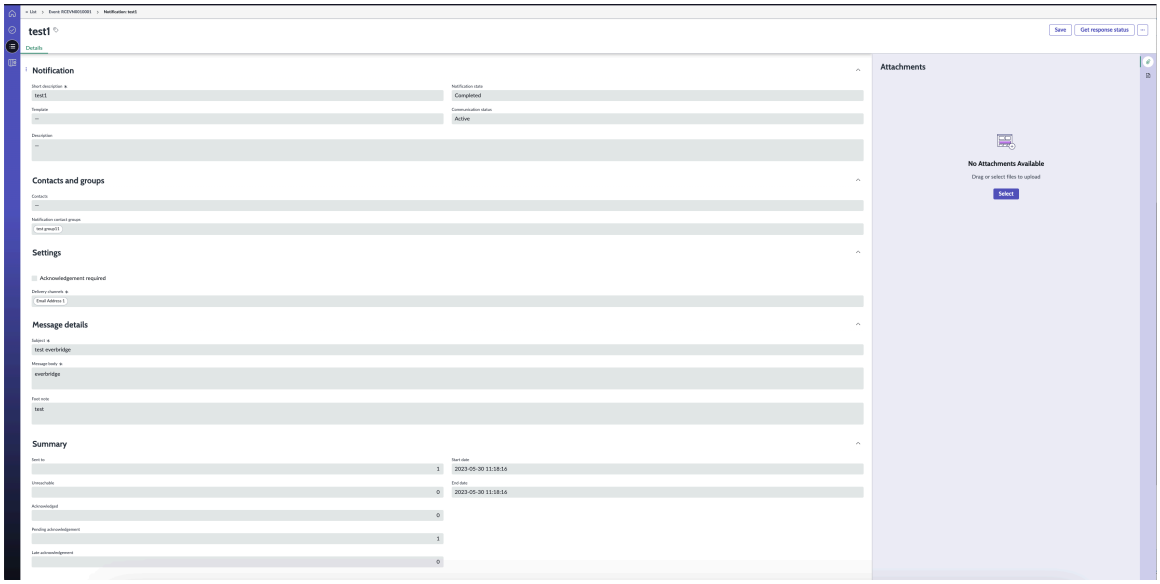
When you send an emergency notification from the Business Continuity Workspace, the action creates an incident and a notification for the incident in Everbridge to be sent to the right contacts and groups.

The emergency notifications for an event are displayed on the **Emergency notifications** tab for the event. You can view the details of the emergency notification such as the notification state, start date, end date, and so on as shown in the following example.




The emergency notification form is shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## Summary of the notification sent to contacts

The **Summary** section in the notification form displays a list of the contacts and groups to whom the notification was sent and their responses are also recorded. It also displays the number of contacts who could not be reached, the number of contacts who acknowledged the notification, and the number of pending acknowledgments. This information is retrieved from Everbridge and it is displayed in your Business Continuity Workspace as shown in the following example.

### Summary of the notification sent to the contacts




The Summary section in the notification form contains the following information:

Sent to

Number of contacts to whom the notification was sent.

Unreachable

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Number of contacts to whom notification was not sent.

Acknowledged

Number of contacts who acknowledged the receipt of notification.

Pending acknowledgment

Number of contacts who did not acknowledge the receipt of notification.

Late acknowledgment

Number of contacts who confirmed the receipt of notification after the notification duration had elapsed.

If there are many contacts to whom the notification could not be delivered, then you can create another notification for the same crisis event. This time, you can send it to a team of managers, as the previous notification did not reach many contacts.

### Administrative tasks for integrating Crisis Management with Everbridge

For information on the administrative tasks for integrating Crisis Management with Everbridge notifications system, see Setup for Everbridge notifications.

## Configuring Business Continuity Management

Configure the Business Continuity Management application to perform the business continuity tasks for your organization.

### Configuration overview

Configuring Business Continuity Management involves installing the application from ServiceNow® Store and setting it up by the administrators.

**Note:** If you have the BCM role, you can perform the setup tasks that are described in this section.

- Install the Business Continuity Management application from store. For more information, see Install Business Continuity Management from ServiceNow Store.

  **Note:** Installing GRC: Business Impact Analysis, GRC: Business Continuity Planning, or GRC: Crisis Management automatically installs GRC: Business Continuity Management – Core and GRC: Business Continuity Management – Components.

- Verify that you have assigned users with the required roles. For detailed instructions and a list of roles, see Components installed with Business Continuity Management.
- Set up the Business Continuity Management application by performing the administrative tasks with the BCM administrator role. For more information, see General administration setup for BCM.

  **Note:** You can view **My tasks page configurations** and **Properties** in the **General Administration** setup.

- Complete the setup for a business impact analysis by performing the administrative tasks with the BIA administrator role. For more information, see Setup for a business impact analysis.

  **Note:** When you create a business impact analysis in BCM UIB Workspace, you can assign a BCM lead to the analysis in the BIA form itself.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Complete the setup for a business continuity plan by performing the administrative tasks with the BCP administrator role. For more information, see Setup for a business continuity plan.

  **Note:** When you create a business continuity plan in BCM UIB Workspace, you can assign a BCM lead to the plan in the BCP form itself.

- Format the PDF templates for a business impact analysis, a business continuity plan, or an event. For more information, see Format the PDF templates for BIA, BCP, and Events.
- Configure the 360° relationship registries and views. For more information, see Configure 360° relationship registries and views.
- Set up the notifications with Everbridge. For more information, see Setup for Everbridge notifications.
- Set up the Crisis map. For more information, see Setup for Crisis map.
- Review the setup tasks that are performed by an administrator. For more information, see Setup by system administrators.
- Review the setup information for UI Builder. For more information, see Setup for the UI Builder.

**Note:**

Both BCM classic Workspace and BCM Configurable Workspace use the Workspace view. If you have made any customizations in other UI views, you must apply the same customizations before or after upgrading from a prior release to the Utah release. For more information, see the KB1442692 article.

For information on the custom components configuration in BCM classic Workspace, see the KB1442692 article.

For information on how to migrate reports and custom changes to BCM Configurable Workspace, see the KB1444397 article.

## Business Continuity Management and the ServiceNow Store

Business Continuity Management applications are available from the ServiceNow Store, enabling you to obtain new and updated features more rapidly. Before you can use the Business Continuity Management applications, you must verify that you have an entitlement to use them.

## Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

The list of BCM applications available on ServiceNow Store is:

| Application | Description |
|---|---|
| GRC: Business Impact Analysis | Provides structured workflows for business continuity management teams to assess the impact of a disruption for critical resources such as business processes, applications, and locations. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Application | Description |
|---|---|
| GRC: Business Continuity Planning | Provides capabilities for business continuity management teams to create, review, and approve business continuity and disaster recovery plans. |
| GRC: Crisis Management | Provides capabilities for business continuity management teams to activate business continuity plans during plan exercises and actual crisis events. |
| GRC: Crisis Management integration with Everbridge Notifications (com.snc.bcm.app_crisis_ebn_intg) | Provides integration with Everbridge to create and send notification, and track responses. |
| GRC: Crisis Map (com.snc.app_bcm_crisis_map) | Provides the ability to integrate with the Feeds and Alert Management application to view the threat alerts and assets at risk on the BCM crisis map. Also, take appropriate action by triggering the Crisis Management event and notification workflows. |
| GRC: Approver Configurator (sn_grc_appr) | Provides capabilities to define multiple levels of approvals based on approval rule definitions. |

**Note:** Installing GRC: Business Impact Analysis, GRC: Business Continuity Planning, or GRC: Crisis Management automatically installs GRC: Business Continuity Management – Core, GRC: Business Continuity Management – Components, and GRC: Approver Configurator.

GRC: Business Continuity Management – Core provides capabilities to configure data that are required for the business continuity management applications. This application also installs GRC: Business Continuity Management – Components: Now Design System components for Business Continuity Management application.

### Get entitlement for the Business Continuity Management application

The first step in installing an application is to verify that the application or the product and its associated applications have valid ServiceNow entitlements.

#### Before you begin

Role required: admin

Individuals performing entitlement must have a Now Support account and have permission to request applications for the instances under consideration.

#### Procedure

1. Navigate to the ServiceNow Store.
2. Select **Login** and log in using your Now Support credentials.
3. Select the **ServiceNow Products** tab to view all available ServiceNow Store products. Integrations and other types of content are shown on the **Certified Apps** tab.
4. Select the product name of the product that you are getting entitlement to. All applications associated with the product you are entitling are listed. When you have obtained entitlement to the core product, the applications listed under it are also entitled.
5. Select **Opt-in** to verify that you have entitlement to the product and the applications listed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You are prompted to read and accept the ServiceNow Store terms and conditions.

6. Select the check box and select **Accept**.

   **Note:** A check mark appears next to the product name and the **Manage Entitlements** button appears.

   The check mark indicates that you have subscribed to the product and its associated applications. It is time to manage your entitlements. This is a one-time process for this product and any other products that you want to install in the future.

7. You can select **Manage Entitlements** to change the instances affected by the applications to which you are entitled.
   After you have agreed to the ServiceNow Store Terms and Conditions and managed entitlements, you can entitle other products by selecting the plus sign (+) next to the product name.

   You are now ready to install the application.

### Install Business Continuity Management from ServiceNow Store

You can install the Business Continuity Management application if you have the admin role. This application includes demo data and installs the related store applications if they are not already installed.

#### Before you begin

Role required: admin

In the ServiceNow Store, you must ensure that you have entitlements (or licenses) to the application and its dependent applications.

#### Procedure

1. Navigate to **System Applications** > **All Available Applications** > **All**.
2. Find the Business Continuity Management application using the filter criteria and search bar.

   You can search for the application by its name or ID. If you cannot find an application, you may have to request it from the ServiceNow Store.

   Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

3. Select **Install**.
4. In the Application installation dialog box, review the application dependencies.

   If your application requires other applications, install them first if they are not already installed.

   Installing your application automatically installs the dependent applications if they are not installed already.

5. If demo data is available and you want to load it, select **Load demo data**.

   Some applications include demo data, which are sample records that describe application features for common use cases. Load demo data when you first install the application on a development or test instance.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** If you do not select the **Load demo data** check box for a store application during installation, demo data is not available to install from the **Application Manager** later. For information on how to install or reinstall demo data after the initial installation, see the Workaround to install demo data if application is already installed [KB0722909] article in the HI Knowledge Base.

6. Select **Install**.

**Note:** Installing GRC: Business Impact Analysis, GRC: Business Continuity Planning, or GRC: Crisis Management automatically installs GRC: Business Continuity Management – Core and GRC: Business Continuity Management – Components.

### Business Continuity Management lite operators

The Business Continuity Management application provides flexible user licensing terms. The terms are based on whether your operator has read-only access or can complete certain types of tasks.

## Overview of the lite operator classification

The Business Continuity Management roles that classify as lite operators are users who are responsible for the following tasks:

- Respond to the business impact analysis (BIA) plans when they are added as the contributors to the business impact analysis.
- Approve the assigned approval record from the record in the Lists view or My tasks page.

To enable lite operators to respond to tasks, you must assign them with the appropriate role for the activity and add them to the record as an approver. When this criteria is met, the lite operator can approve or reject a record and provide workflow notes.

For detailed information that describes how to configure BCP or BIA plan templates, see Configure a business continuity plan template for your business and Configure a business impact analysis (BIA) template.

For information about all roles that are installed with the activation of the Business Continuity Management application, see Components installed with Business Continuity Management.

## BCM lite operator role

The BCM lite operator role (sn_bcm_lite.lite_operator) contains the roles listed in the following table.

**BCM lite operator role classification**

| Role | Description | Additional Information |
|---|---|---|
| sn_bcm_contributor | Enables the user to respond to BIAs in which they are tagged as a contributor. | The BIA owner must add the user as a contributor to the BIA. |
| sn_bcm.core_viewer | Enables the user to view the BIA, plans, exercises, and events in the workspace UI. | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**BCM lite operator role classification (continued)**

| Role | Description | Additional Information |
|---|---|---|
| sn_bia.bia_contributor | Enables the user to respond to BIAs in which they are tagged as a contributor. | The BIA owner must add the user as a contributor to the BIA. |
| sn_bcm.recovery_team_member | Enables the user to receive and respond to the assigned recovery tasks. | |
| sn_bcm_viewer | Enables the user to view all records in the BCM application. | |
| sn_bcp.plan_viewer | Enables the user to view the plans in a read-only format. | |
| sn_bia.bia_viewer | Enables the user to view the BIA responses in a read-only format. | |
| sn_recovery.event_viewer | Enables the user to view an exercise or event in a read-only format. | The read-only information is needed so that the recovery event member has the context of the entire exercise though the user can only respond to assigned tasks. |
| sn_crisis_ebn.viewer | Enables the user to view emergency notifications in a read-only format. | |
| sn_recovery.event_member | Enables the user to receive and respond to the assigned recovery tasks during an exercise or event. | Recovery tasks must be assigned to the recovery team member. |

## BCM roles that you can't assign to your lite operators

Operator roles can't be assigned to lite operators. If you assign a role to a user, it counts the user as an operator and you no longer have a flexible licensing model.

You can't assign the following roles to your lite operators:

- sn_bia.bia_admin
- sn_bia.bia_manager
- sn_bia.bia_planner
- sn_bcp.plan_admin
- sn_bcp.plan_manager
- sn_recovery.event_manager
- sn_recovery.event_user
- sn_crisis_ebn.admin
- sn_crisis_ebn.user

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For additional information on role assignments, see the GRC Business User Role [KB0864247] article in the Now Support Knowledge Base.

**Note:** You must log in to Now Support to view the articles.

## Lite operator activities and limitations

The following table describes the lite operator activities and limitations.

**BCM lite operator activities and limitations**

| Activity | Description | Create | Read | Update | Approve |
|---|---|---|---|---|---|
| Business impact analysis (BIA) | • Respond to the BIA analysis.<br>• View a completed analysis.<br>• Participate in the BIA workflow.<br>• Review the analysis and then approve or reject it. | | X | X | X |
| Business continuity planning (BCP) | • View and download the published continuity and disaster recovery plans.<br>• Participate in the plan workflow.<br>• Review and approve or reject an analysis. | | X | | X |
| Business continuity exercises | • View the exercise details.<br>• Participate in the | | X | | X |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**BCM lite operator activities and limitations (continued)**

| Activity | Description | Create | Read | Update | Approve |
|---|---|---|---|---|---|
| | recovery tasks.<br>• Participate in the exercise results workflow.<br>• Review and approve or reject an analysis. | | | | |
| Crisis events | • Report and view the crisis details.<br>• Participate in the recovery tasks.<br>• Participate in the exercise results workflow.<br>• Review and approve or reject an analysis. | | X | | X |
| Update recovery tasks status | • Receive the recovery tasks from the exercises and crisis events.<br>• Report the progress and status back to your event coordinator. | | X | X | X |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**BCM lite operator activities and limitations (continued)**

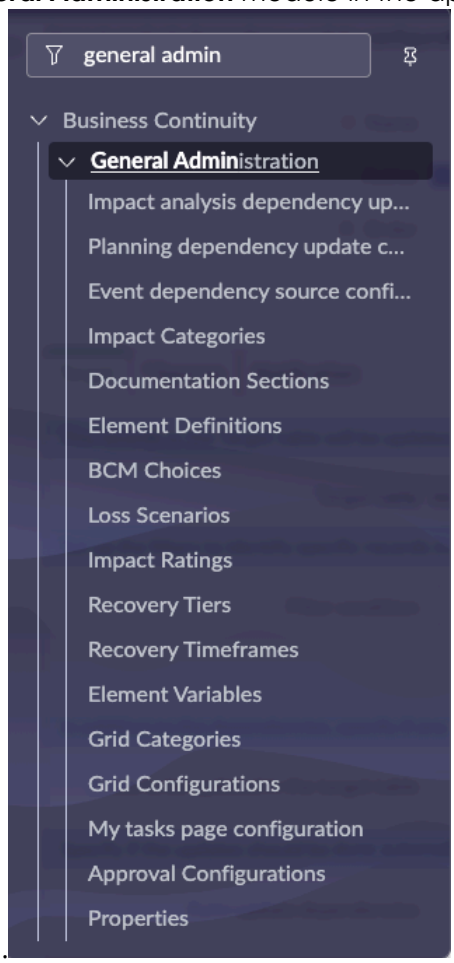
| Activity | Description | Create | Read | Update | Approve |
|---|---|---|---|---|---|
| Emergency notification template | • View the emergency notifications.<br>• Participate in the workflow. | | X | | X |

## General administration setup for BCM

If you are the BCM administrator, you can set up the Business Continuity Management application by performing certain administrative tasks.

## General Administration module

The administrative tasks that are associated with the BCM application are listed in the **General Administration** module in the application UI as shown in the following example.




The Business Continuity Management administrator with the sn_bcm.admin role is responsible to perform the administrative tasks that are associated with the Business Continuity Management application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Typically, the Business Continuity Management administrator performs the following administrative tasks:

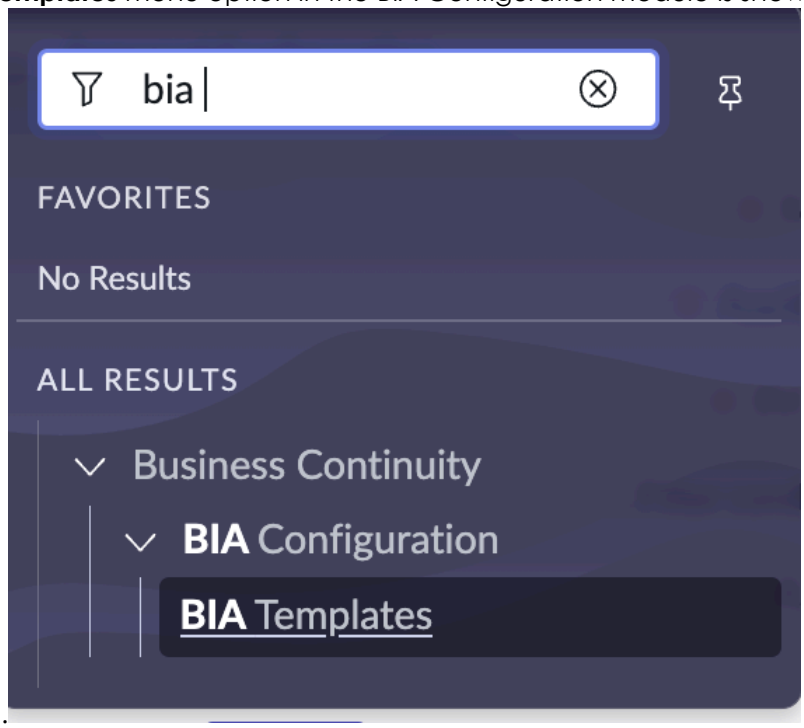
- Configure the impact categories. For more information, see Configure an impact category for the business impact analysis.
- Configure the documentation sections. For more information, see Configure the documentation section for a business continuity plan.
- Configure the element definitions. For more information, see Configure an element definition for the business impact analysis.
- Configure the loss scenarios. For more information, see Configure a loss scenario in your business continuity plan.
- Configure the impact ratings. For more information, see Configure an impact rating to assess the impact category.
- Configure the recovery tiers. For more information, see Configure a recovery tier for the business impact analysis.
- Configure the recovery timeframes. For more information, see Set up a recovery timeframe for a recovery tier.
- Configure the element variables. For more information, see Configure an element variable for an element definition.
- View the My tasks page configurations module. For more information, see My tasks page configurations.
- Configure the approval configurations. For more information, see Approval configuration.
- Configure the properties. For more information, see BCM properties.
- For more information on the grid configurations and categories, see Configure the grid for the BIA dependency assessment and Configure a grid category for the grid configuration.

## BIA Configuration module

The BCM administrator configures the BIA templates in the BIA Configuration module. Configuring the BIA templates is a pre-requisite for performing the business impact analysis.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

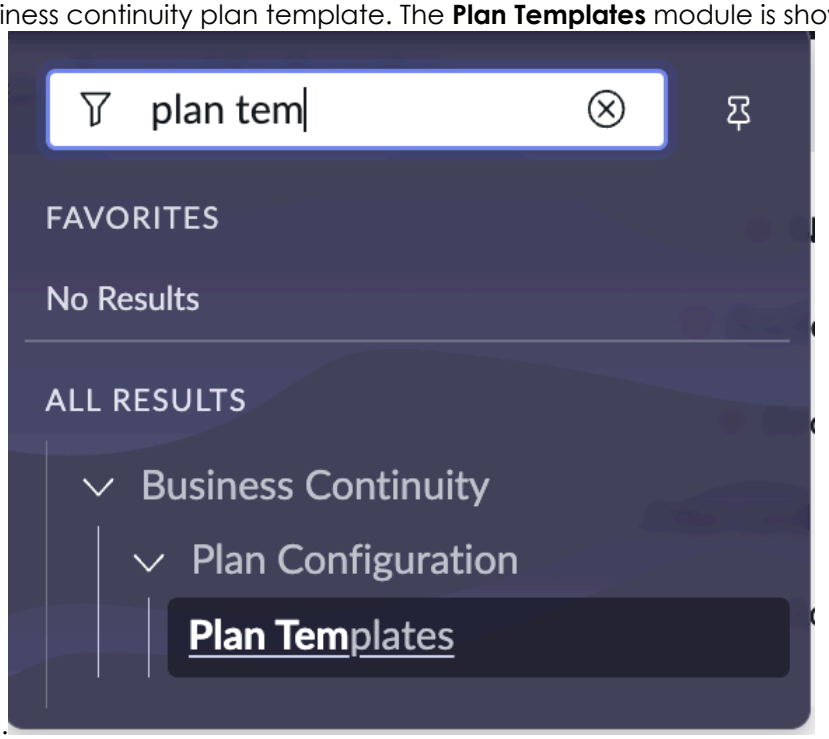
The **BIA templates** menu option in the BIA Configuration module is shown in the following example.




For more information on configuring a BIA template, see Configure a business impact analysis (BIA) template.

### Plan Templates module

Typically, the Business Continuity Management administrator uses the **Plan Templates** module to configure a business continuity plan template. The **Plan Templates** module is shown in the following example.




For more information on configuring a business continuity plan template, see Configuring the plan template for the business continuity plan.

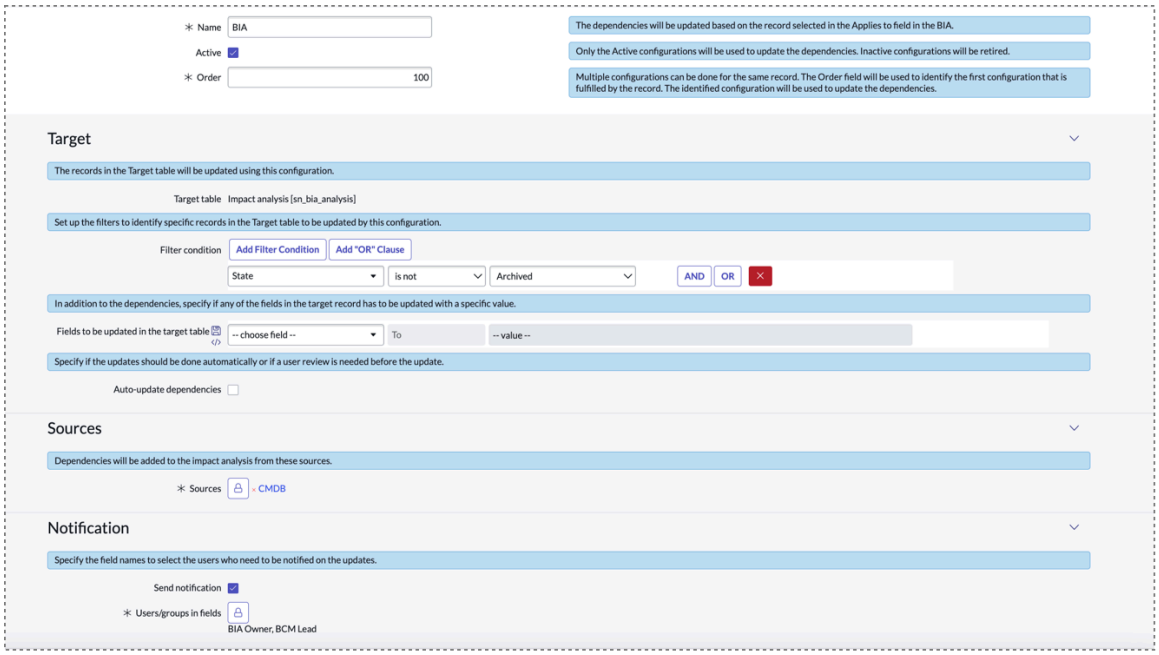
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Configuring the impact analysis dependency updates

The BCM administrators configure the Impact analysis dependency update configuration module so that an auto-update of the BIA dependencies can be scheduled based on the source data and relationships in the CMDB.

## Impact analysis dependency update configuration module

The BCM administrators access the Impact analysis dependency update configuration module by navigating to **General Administration** in the application UI. The module contains the configuration details such as the name, order, target records, sources, and notification preferences as shown in the following example.




## Configure the sources for adding the dependencies

Configure the sources for fetch the latest dependencies of the BIA in the Impact analysis dependency update configuration module. A source is created for CMDB that is used to read the CMDB dependencies. The **Applies to** field of the BIA is the input asset. It gets the dependencies from CMDB, based on whatever is your BIA is done on.

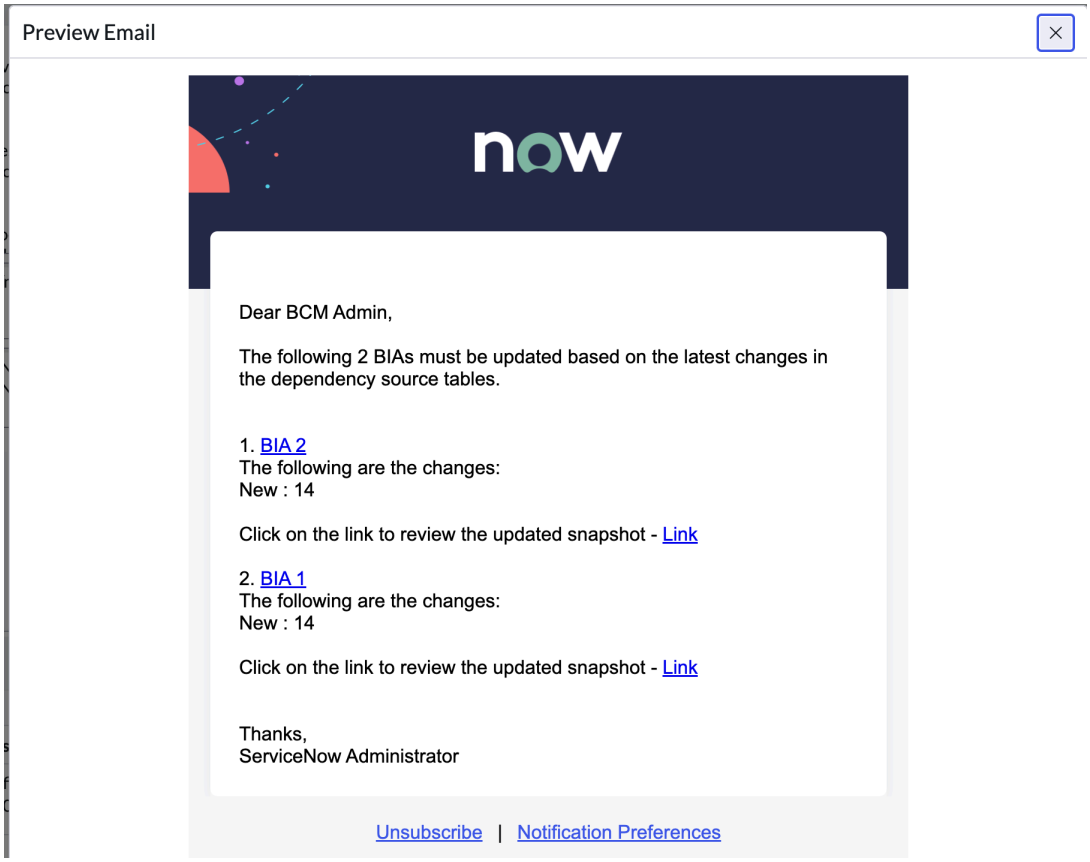
**Note:** You can fetch the latest dependencies of the BIAs from the CMDB relationships only.

## Auto-update the dependencies and set the notification preferences

The BCM administrators select the **Auto-update dependencies** option to schedule an auto-update of the dependencies in the BIAs.

The BCM administrators select the **Send notification** option to notify the BIA owners about the updated dependencies. The email notification contains the details of the dependency updates for the BIA records as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The snapshot records are displayed in the Pending updates module of the BIA from the list view. The delta snapshot record displays details of the BIA and updated dependency configuration such as Added, Updated, and Deleted assets for the BIA.

BIA owners then update the CMDB assets and dependencies manually by selecting the **Update dependencies** UI action displayed in the Dependency assessment of the BIA. The BIA owners or BIA approvers then review the dependency updates and save the changes to the BIA.

For more information on configuring the Impact analysis dependency update configuration module, see Configure the Impact analysis dependency update configuration module.

### Configure the Impact analysis dependency update configuration module

Configure the Impact analysis dependency update configuration module to configure the BIA record (for which the dependencies are updated), its target records, sources, and notification preferences.

#### Before you begin

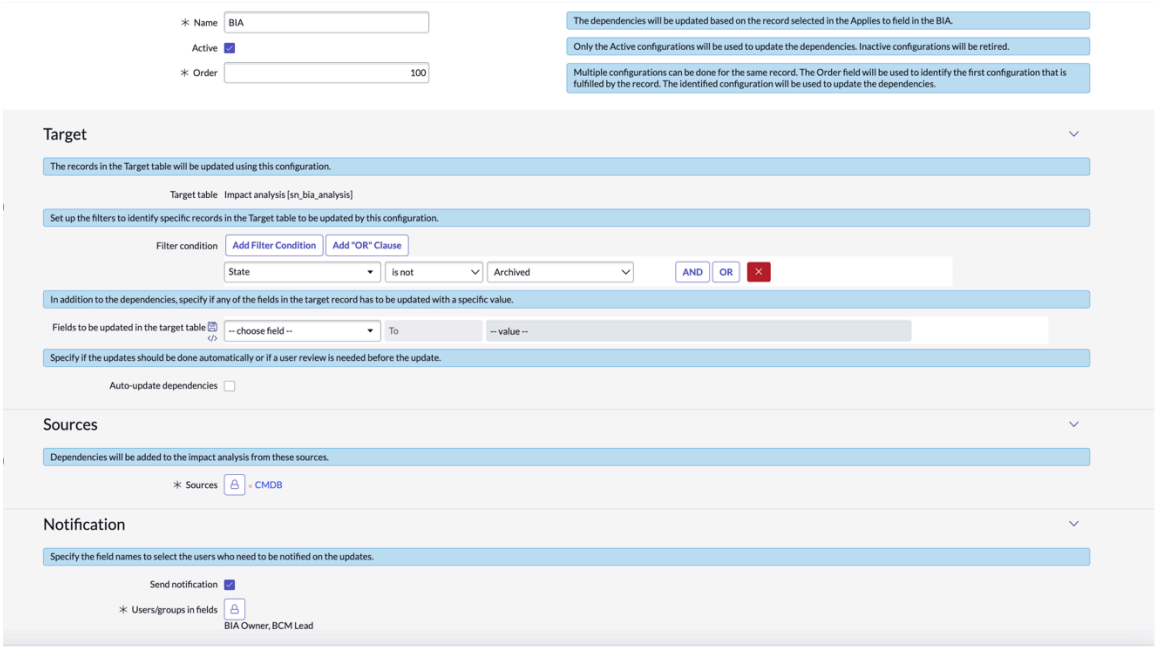
Role required: sn_bcm.admin

#### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Impact analysis dependency update configuration**.
2. Select **New**.

   The following example shows the Impact analysis dependency update configuration module.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. On the form, fill in the fields.

   For more information on the fields in the form, see Impact analysis dependency update configuration form.

4. Select **Submit**.

   According to the configuration set up by the BCM administrator in the Impact analysis dependency update configuration module, the dependencies are updated in the BIA.

   The BIA owner and approver review the updated dependencies and complete the BIA workflow. For more information on scheduling an auto-update of the dependencies in the BIA, see Schedule an auto-update of the dependencies in the business impact analysis.

### Impact analysis dependency update configuration form

Use the Impact analysis dependency update configuration form to configure the details of the dependency updates such as the BIA record name, target records, sources, and notification preferences.

## Impact analysis dependency update configuration record form

For a description of the field values, see the following table.

**Impact analysis dependency update configuration record form**

| Field | Description |
|---|---|
| Name | Name of the dependency update configuration rule. |
| Active | Option to select the active configurations. Active configurations are used to update the dependencies. Inactive configurations are retired. |
| Order | Field to identify the first configuration that is fulfilled by the record. The identified |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Impact analysis dependency update configuration record form (continued)**

| Field | Description |
|---|---|
| | configuration is used to update the dependencies. Multiple configurations can be done for the same record. When the filter conditions are the same, the least order such as 0 takes the preference. |
| Target | |
| Target table | Impact analysis [sn_bia_analysis] table that contains the BIA records. These records are updated according to the configuration set up in the Impact analysis dependency update configuration module. |
| Filter condition | Filter conditions to identify specific records in the target table. These records are updated according to the configuration set up in the Impact analysis dependency update configuration module. |
| Fields to be updated in the target table | Fields in the target record that can be updated with a specific value in addition to the dependencies. |
| Auto-update dependencies | Option to update the dependencies automatically. BCM administrators can specify if the updates should be done automatically or if a user review is needed before the update. |
| Sources | |
| Sources | Applicable sources for adding dependencies to the impact analysis. For the BIA record, the source used is CMDB. |
| Notification | |
| Send notification | Option to notify the users or user groups on the updates. |
| Users/groups in fields | Option to select the users or groups fields in sn_bia_analysis who should receive a notification about the updates. For example, you can select the BIA owner and BCM lead to receive the updates. |

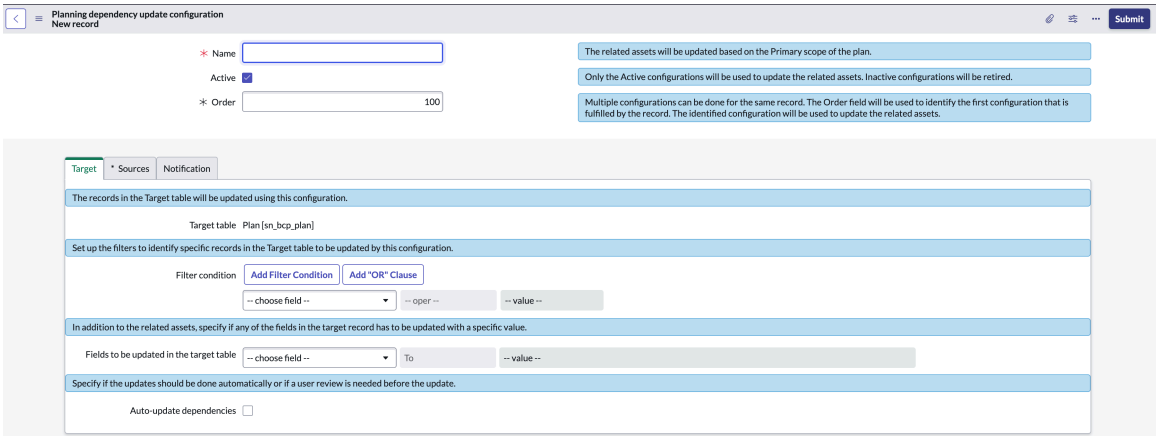
### Configuring the planning dependency updates

The BCM administrators configure the Planning dependency update configuration module so that an auto-update of the related assets in the plans can be scheduled based on the source data and relationships in the CMDB and BIA.

## Planning dependency update configuration module

The BCM administrators configure details of the plan record, its target records, sources, and notification preferences in the Planning dependency update configuration module as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



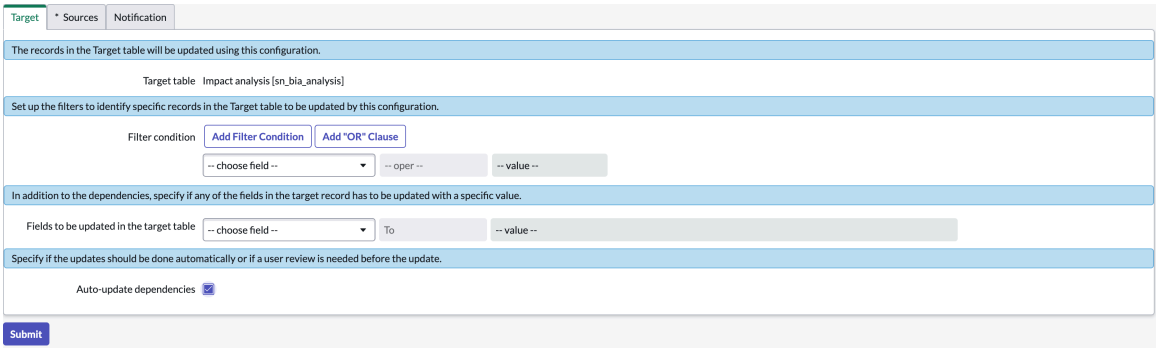

## Configure the sources for fetching the dependencies

The BCM administrators configure the sources for fetching the latest dependencies of the plan from different sources such as BIA upstream dependency, BIA downstream dependencies, and CMDB.

**Note:** In the plans, the dependencies are fetched for all primary scope assets.

## Auto-update the dependencies

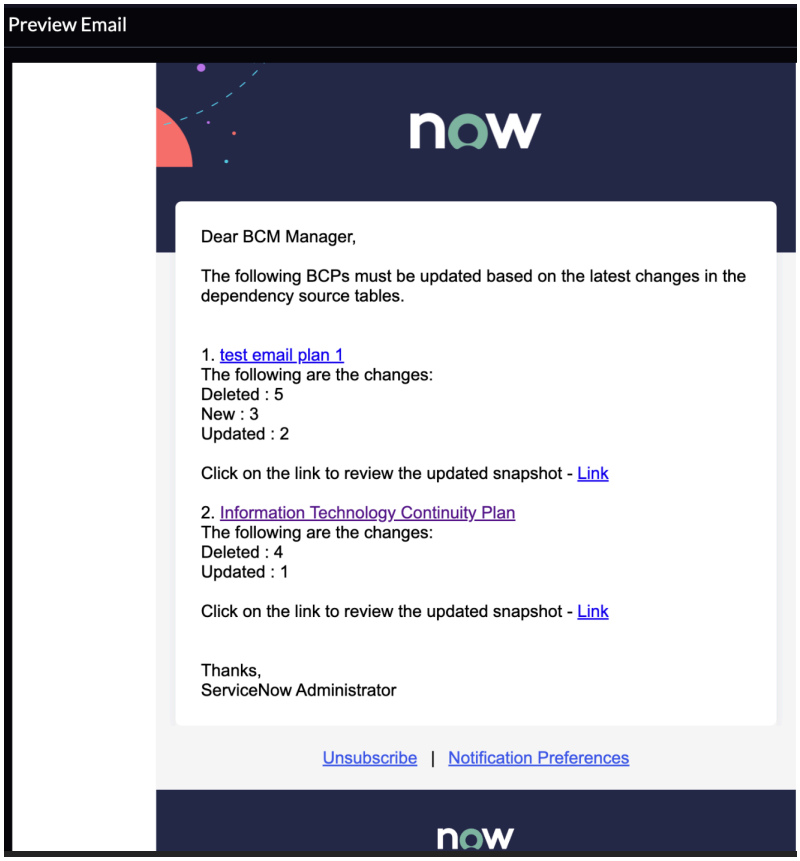
The BCM administrators select the **Auto-update dependencies** option to schedule an auto-update of the related assets in the plans as shown in the following example.




## Set the notification preferences

The BCM administrators select the **Send notification** option to set the notification preferences for the plan owners. For every planning dependency update, an automated email is sent to the plan owners about the planning dependency updates and links to the updated snapshot records as shown in the example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The plan owner and BCM lead reviews the dependency updates from the snapshot record. The delta snapshot record displays the updated dependencies such as Added, Updated, and Deleted assets for the selected plan record.

For more information on configuring the Planning dependency update configuration module, see Configure the Planning dependency update configuration module.

### Configure the Planning dependency update configuration module

Configure the Planning dependency update configuration module to configure the plan record (for which the dependencies are updated), its target records, sources, and notification preferences.

#### Before you begin

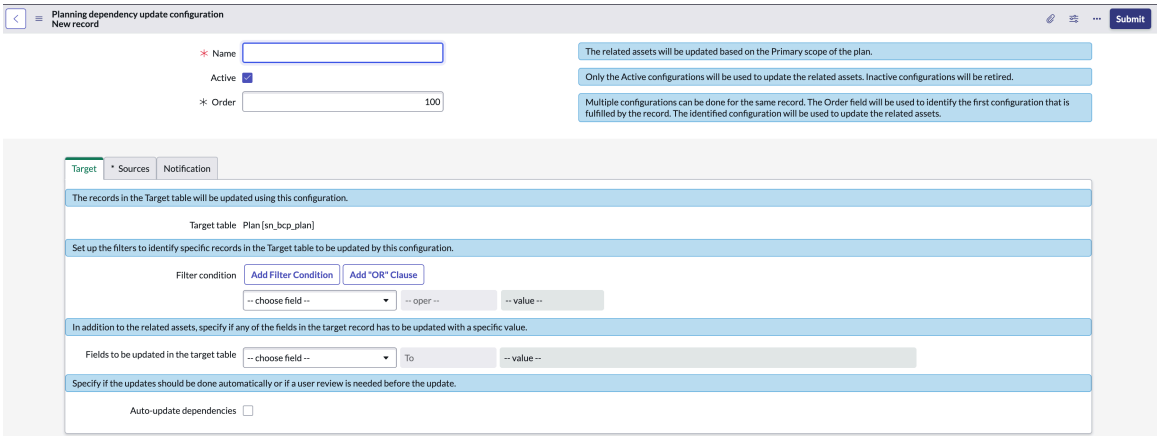
Role required: sn_bcm.admin

#### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Planning dependency update configuration**.
2. Select **New**.

   The following example shows the Planning dependency update configuration module.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. On the form, fill in the fields.

   For more information on the fields in the form, see Planning dependency update configuration form.

4. Select **Submit**.

   As per the sources and preferences set up by the BCM administrator in the BCM administrator in the Planning dependency update configuration module, the planning dependency updates are auto-updated for the plan record.

   The BCP owner and approver review the updated dependencies and complete the BCP workflow.

### Planning dependency update configuration form

Use the Planning dependency update configuration form to configure the plan record, its sources, and preferences such as the plan record name, sources, and notification preferences and schedule an auto-update of the related assets in the plans.

## Planning dependency update configuration record form

For a description of the field values, see the following table.

**Planning dependency update configuration record form**

| Field | Description |
|---|---|
| Name | Name of the plan record. The related assets are updated based on the primary scope of the plan record. |
| Active | Option to select the active configurations. Active configurations are used to update the dependencies. Inactive configurations are retired. |
| Order | Field to identify the first configuration that is fulfilled by the record. The identified configuration is used to update the dependencies. Multiple configurations can be done for the same record. |
| Target | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Planning dependency update configuration record form (continued)**

| Field | Description |
|---|---|
| Target table | Plan [sn_bcp_plan] table that contains the plan records. These records are updated as per the configuration set up in the Planning dependency update configuration module. |
| Filter condition | Filter conditions to identify specific records in the target table. These records are updated as per the configuration set up in the Planning dependency update configuration module. |
| Fields to be updated in the target table | Fields in the target record that can be updated with a specific value. |
| Auto-update dependencies | Option to update the dependencies automatically. BCM administrators can specify if the updates should be done automatically or if a user review is needed before the update. |
| Sources | |
| Sources | Applicable sources for adding related assets to the plan. For the business continuity plan record, the following sources are used:<br>• BIA Upstream<br>• BIA Downstream<br>• CMDB |
| Notification | |
| Send notification | Option to notify the users or user groups on the updates. |
| Users/groups in fields | Option to select the users or groups who should receive a notification about the updates. For example, Plan owner and BCM lead are selected to receive the updates. |

### Add the dependencies of the impacted assets manually in the events

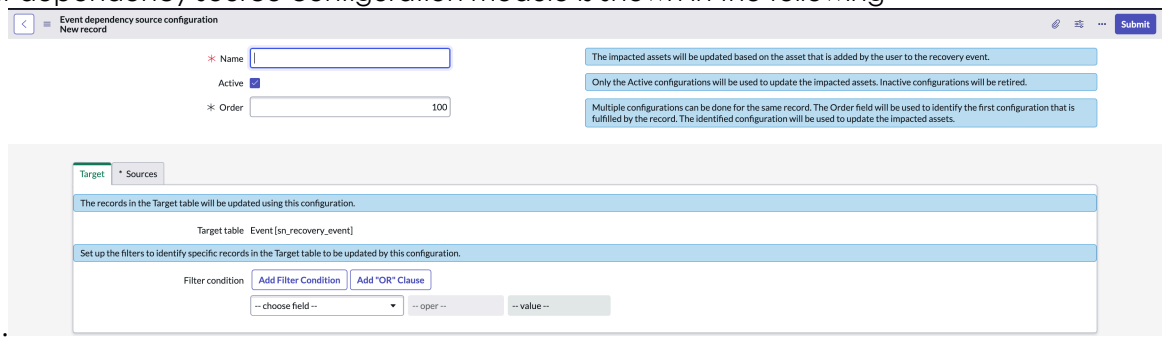
You can add the dependencies of the impacted assets in the events and exercises based on the source data and relationships in the CMDB, BIAs, and plans.

## Configuring the sources in the Event dependency source configuration module

The BCM administrators can configure the sources to get the event dependencies in the Event dependency source configuration module.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Event dependency source configuration module is shown in the following example.




When the BCM administrators can update the target records, filter condition for the records, and sources to fetch the event dependency.

Dependencies are added in the events only when the user selects the **Update dependencies** UI action. Dependencies are fetched from the following sources for the events:

- BIA upstream dependency
- BIA downstream dependencies
- CMDB
- Plan primary assets
- Plan related assets

**Note:** In an event, the dependencies of all assets are added manually where the source is Manual.

Setting up the Event dependency source configuration module is a one-time activity. Once the sources are configured in the Event dependency source configuration module, the updates are synchronized in the events.

For more information on setting up the Event dependency source configuration module, see Configure the Event dependency source configuration module.

## Roles associated with event dependency updates

Users with the following roles typically check for the dependency updates in an event:

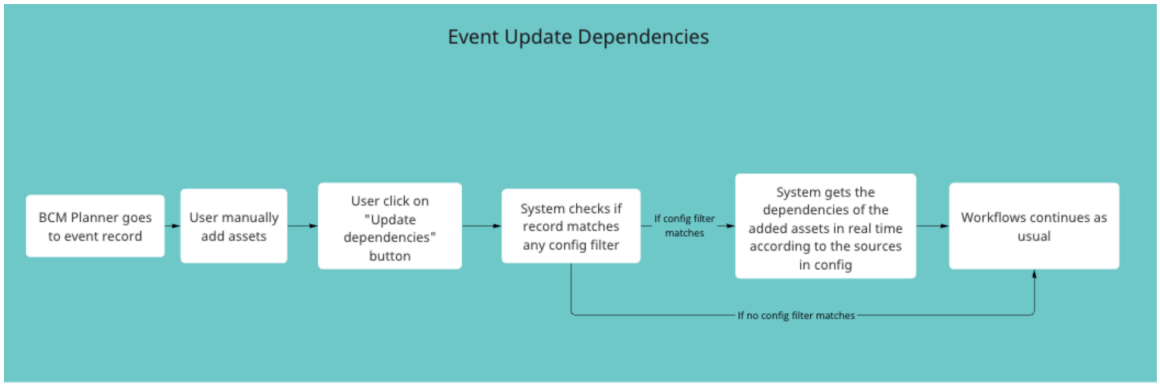
- The BCM program managers, BCM planners, and BCM managers can update the latest dependencies.
- BCM administrators can configure the Event dependency source configuration module.

## Workflow for updating the dependencies manually in the events and exercises

As the BCM application user, when you select the **Update dependencies** UI action in the Event record, the dependencies of all assets are added manually where the source is Manual.

The BCM application executes a workflow to update the impacted assets in the events and exercises as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




1. The BCM planner navigates to the event record.
2. The BCM planner selects the **Update dependencies** UI action to add the assets manually.
3. The application checks if the event record matches any configuration filter.
4. If the event record matches any configuration filter, the system gets the dependencies of the added assets in real time according to the sources defined in the configuration (Event dependency source configuration module).
5. If the event record does not match any configuration filter, the events workflow then continues for the next steps, the events workflow then continues for the next steps.

For more information on updating the event dependencies manually, see Update the event dependencies manually.

## Data Relationships Framework

Beginning with the Utah release, the Data Relationships Framework application (com.sn_app_grc_relationship_config) supports the BCM application with the underlying framework to add the dependencies of the impacted assets in the events and exercises. The Data Relationships Framework application is installed with the BCM application by default.

For more information on the Data Relationships Framework, see Data Relationships Framework.

### Configure the Event dependency source configuration module

Configure the sources for adding the event dependencies in the Event dependency source configuration module.

#### Before you begin

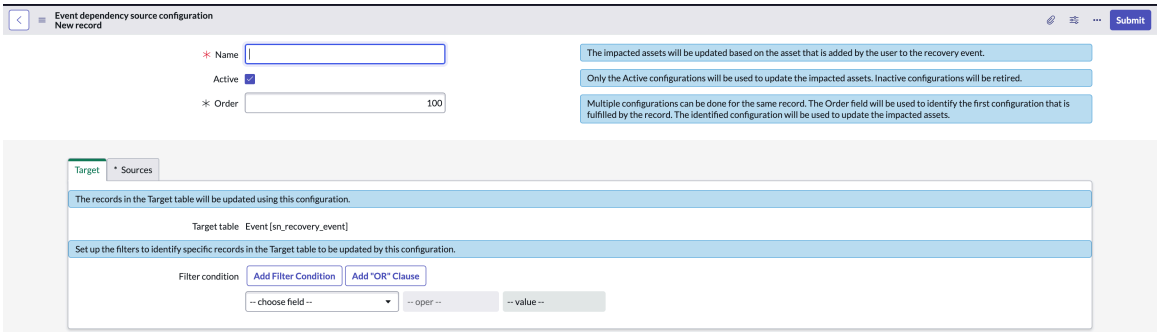
Role required: sn_bcm.admin

#### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Event dependency source configuration**.
2. Select **New**.

   The following example shows the Event dependency source configuration module.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. On the form, fill in the fields.

   For more information on the fields in the form, see Event dependency source configuration form.

4. Select **Submit**.

   As per the sources set up by the BCM administrator in the Event dependency source configuration module, the dependencies are added in the event.

### Event dependency source configuration form

Use the Event dependency source configuration form to add the event dependency details such as the event record name, its target records, and sources in the BCM application.

## Event dependency source configuration record form

For a description of the field values, see the following table.

**Event dependency source configuration record form**

| Field | Description |
|---|---|
| Name | Name of the recovery event. The impacted assets are updated based on the asset that is added by the user to the recovery event. |
| Active | Option to select the active configurations. Active configurations are used to update the dependencies. Inactive configurations are retired. |
| Order | Field to identify the first configuration that is fulfilled by the record. The identified configuration is used to update the impacted assets. Multiple configurations can be done for the same record. |
| Target | |
| Target table | Event [sn_recovery_event] table that contains the event records. These records are updated as per the configuration set up in the Event dependency source configuration module. |
| Filter condition | Filter conditions to identify specific records in the target table. These records are updated |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Event dependency source configuration record form (continued)

| Field | Description |
|---|---|
| | as per the configuration set up in the Event dependency source configuration module. |
| Sources | |
| Sources | Applicable sources for adding impacted assets to the recovery event. For the event record, one of the following sources can be used:<br>• BIA upstream dependency<br>• BIA downstream dependencies<br>• CMDB<br>• Plan primary assets<br>• Plan related assets |

## Configure an impact category for the business impact analysis

Configure an impact category for your business, when you are performing the business impact analysis. Use the **Impact Categories** module in the Business Continuity Management application navigator to define the name, criteria that the impact category contributes to, applicable timeframes, maximum RTO value, and so on.

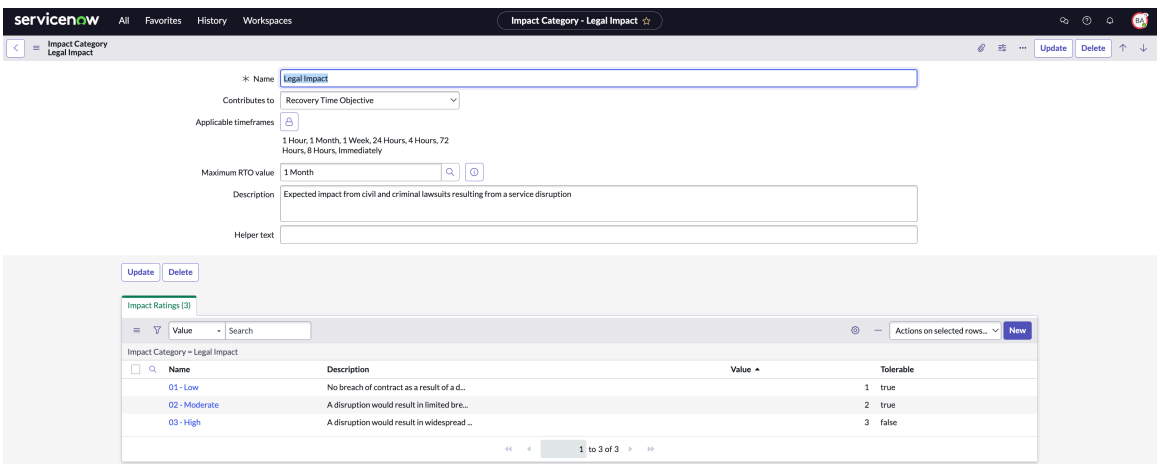
### Before you begin

Role required: sn_bcm.admin

### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Impact Categories**.
2. Select **New**.

   The following example shows the impact ratings that are installed with demo data for an impact category.




3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information on the fields in the form, see Impact Category record form.

4. Select **Submit**.

### Impact Category record form

Use the Impact Category record form to add details about the impact category such as name, criteria that the impact category contributes to, applicable timeframes, maximum RTO value, and so on in BCM UIB Workspace.

## Impact Category record form

For a description of the field values, see the following table.

**Impact Category record form**

| Field | Description |
|---|---|
| Name | Name of the impact category. |
| Contributes to | Contribution to RPO or RTO as a result of the impact on business disruption. If the impact category contributes to Recovery Point Objective, then the Impact analysis questions related list appears. |
| Applicable timeframes | Duration of business process disruption. This field appears only if the **Contributes to** field value is **RTO**. |
| Maximum RTO value | Metric that calculates the maximum time limit within which the business must recover an element after a disruption. |
| Description | Brief description of the impact category. |
| Helper text | Field to add the helper text. It provides a hint to the users on how to respond to the assessment questions. The helper text is then displayed for the user in the business impact analysis record. |

### Configuring the documentation section of the business continuity plan

You can configure the documentation section of a business continuity plan in a structured format. You can describe high level details of the plan such as its purpose, scope, coverage areas, goals, and success criteria.

You can document the details of your business continuity plan in separate documentation sections. You can view the pre-configured documentation sections in the **General Administration** section of the Business Continuity Management application.

When a business continuity plan is created, it populates one or more documentation sections that are selected in the plan template.

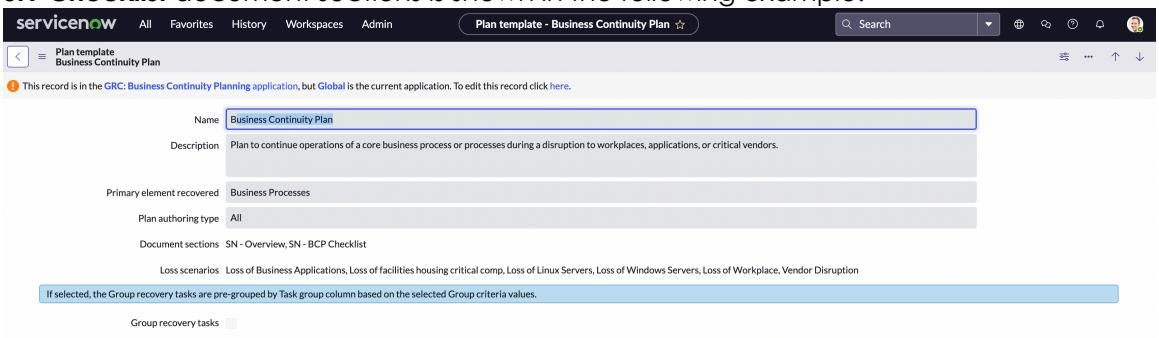
The Business Continuity Management application provides the documentation sections that you are installed with the demo data in the plan template:

- BCP-Assumtions
- BCP-Objectives

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- BCP-Scope
- BIA-Overview
- SN-BCP Checklist
- SN-Overview

A sample **Business Continuity Plan template** with the **SN-Overview** and **SN-Checklist** document sections is shown in the following example.

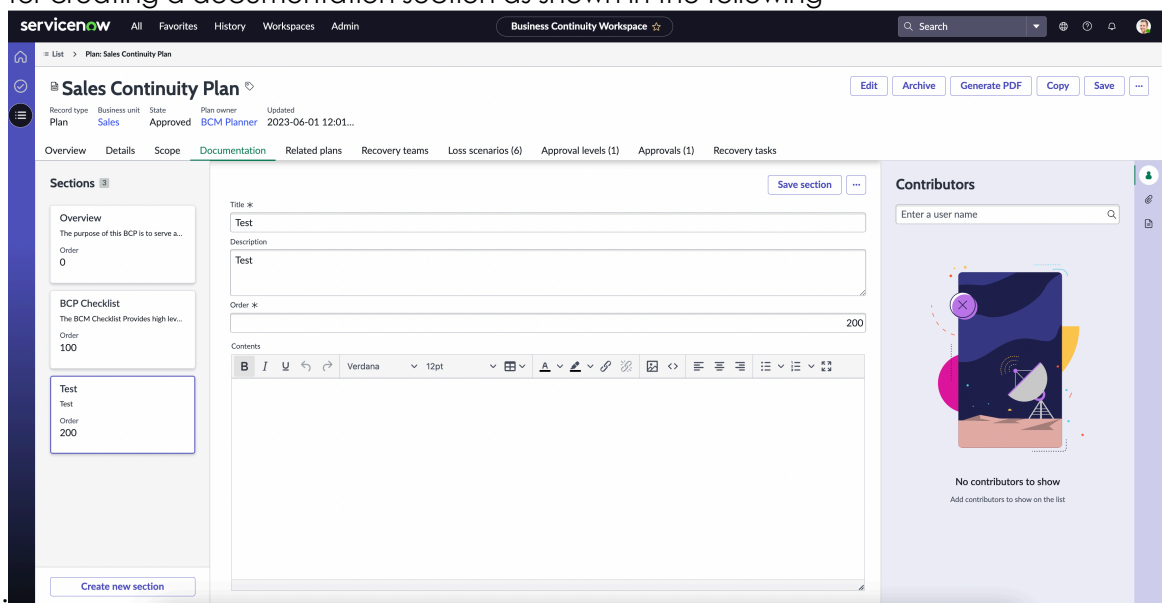



## Creating a documentation section for your business requirement

If you have the BCM administrator role, you can use the documentation section template listed in **General Administration** for creating a documentation section. To configure a documentation section by using the documentation section template, see Configure the documentation section for a business continuity plan.

**Note:** When you create a documentation section in the **Documentation** tab without using the plan template, the **Reset to template** UI action is not available for that documentation section.

You can also create a documentation section on the **Documentation** tab in the Business Continuity Workspace. You can use the **Create new section** UI action for creating a documentation section as shown in the following example.




For more information on creating a documentation section for your business plan in the Business Continuity Workspace, see Create a documentation section.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Configure the documentation section for a business continuity plan

Configure the documentation section of a plan in the Business Continuity Management application. You can use the documentation section to describe a plan in the structured sections such as a checklist of high level details, purpose of the plan, scope describing the plan's purpose and coverage areas, and so on.

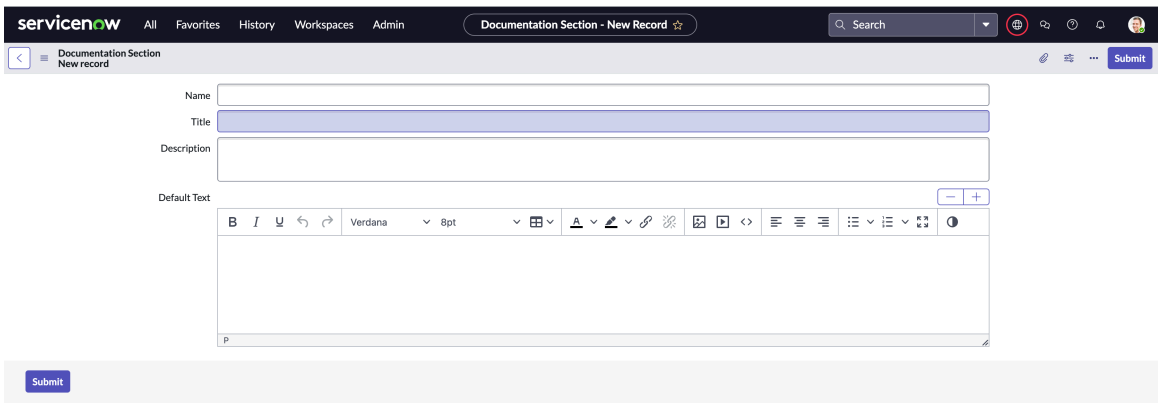
### Before you begin

Role required: sn_bcm.admin, sn_bcp.plan_admin

### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Documentation Sections**.
2. Select **New**.

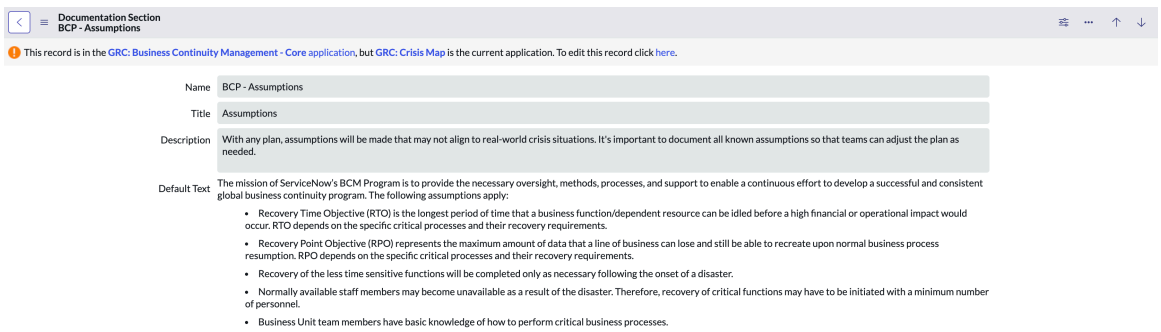
   The documentation section template is shown in the following example.




3. On the form, fill in the fields.

   For more information on the fields, see Documentation Section record form.

   The following example shows the documentation section template from the demo data.




4. Select **Submit**.

## Documentation Section record form

Use the Documentation Section record form to describe a plan in the structured sections in the BCM UIB Workspace.

# Documentation Section record form

For a description of the field values, see the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Documentation Section record form

| Field | Description |
|---|---|
| Name | Name of the documentation section. |
| Title | Documentation section title. |
| Description | Brief description about the documentation section. |
| Default Text | Default text relevant for the documentation section. The text can be edited later when the plan is formulated and the documentation sections are added, in accordance to the plan. |

## Configure an element definition for the business impact analysis

Configure element definitions to identify the configuration item that has to be assessed in a business impact analysis and recovered in a business continuity plan. Use the **Element variables** module in the Business Continuity Management application navigator to configure an element definition.

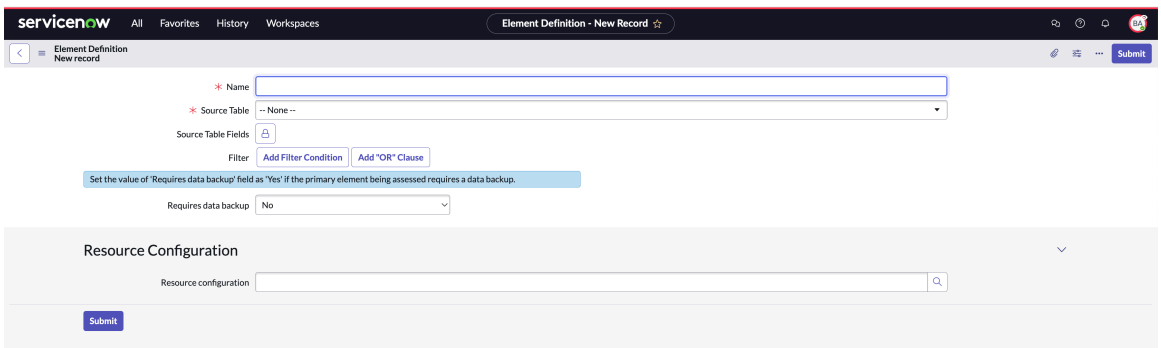
### Before you begin

Role required: sn_bcm.admin

### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Element Definitions**.
2. Select **New**.

   The following example shows the Element Definition record.




3. On the form, fill in the fields.
   For more information on the fields in the form, see Element definition record form.
4. Select **Submit**.

### Element definition record form

Use the Element definition record form to configure a recovery tier with a set of business applications by using BCM UIB Workspace.

## Element definition record form

For a description of the field values, see the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Element Definition record form

| Field | Description |
|---|---|
| Name | Name of the element definition. |
| Source Table | Table that stores the record details of the configuration item. |
| Source Table Fields | Column heads of the source table that you can select for reference. |
| Filter | Add filter condition for the element definition. |
| Requires data backup | Option to indicate if the primary element requires a data backup. Technology assets require data backup as they pertain to important IT information stored in a system or database. |
| Resource configuration | Resource configuration for the element definition. Available options are:<br>• **Location**<br>• **Web Server**<br>• **Datacenters**<br>• **Vendors** |

## Configure an element variable for an element definition

Configure an element variable for a particular dependency of an element. Use the **Element variables** module in the Business Continuity Management application navigator to configure an element variable.

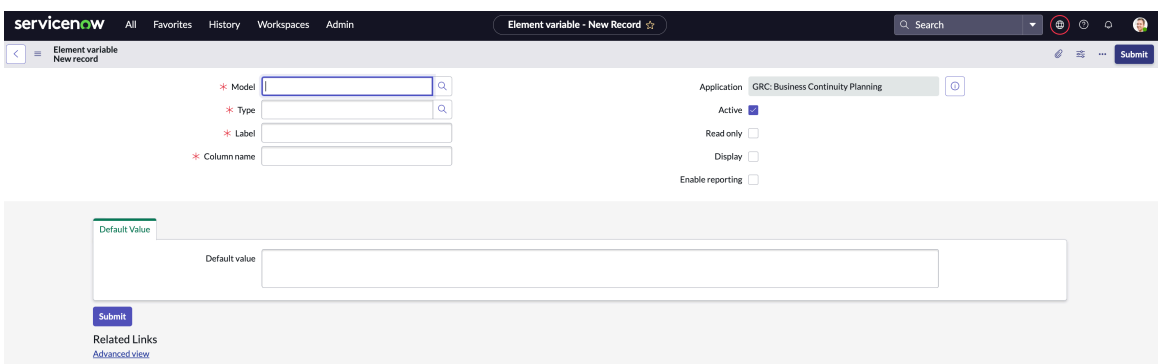
### Before you begin

Role required: sn_bcm.admin

### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Element variables**.
2. Select **New**.

   The following example shows an administrator's view of the element variable record.




3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information on the fields in the form, see Element variable record form.

4. Select **Submit**.

### Element variable record form

Use the Element variable record form to configure an element variable for an element definition by using BCM UIB Workspace.

## Element variable record form

For a description of the field values, see the following table.

**Element variable record form**

| Field | Description |
|---|---|
| Model | Element definition [sn_bcm_element_definition] reference. You can create multiple element variables for an element definition. |
| Type | Field class in the model table. |
| Label | Display name in the dependency group of the BIA dependency grid. |
| Column name | Name of the column in the table. |
| Application | Application that contains the record. |
| Active | Option to activate the element variable. |
| Read only | Option to render the element variable as read only. |
| Display | Option to display the element variable. |
| Enable reporting | Option to report the element variable. |
| Default Value | |
| Default value | Description for the default value. |

### Configure a loss scenario in your business continuity plan

Configure a plan for an identified loss scenario by using the loss scenario template in the Business Continuity Management application. Use the documented plan that has the needs and requirements listed for a potential disaster.

#### Before you begin

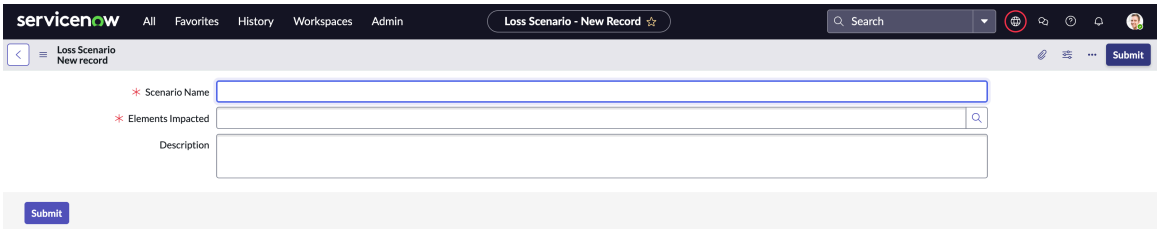
Role required: sn_bcm.admin, sn_bcp.plan_admin

#### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Loss Scenarios**.
2. Select **New**.

The Loss scenario form is shown in the following example.

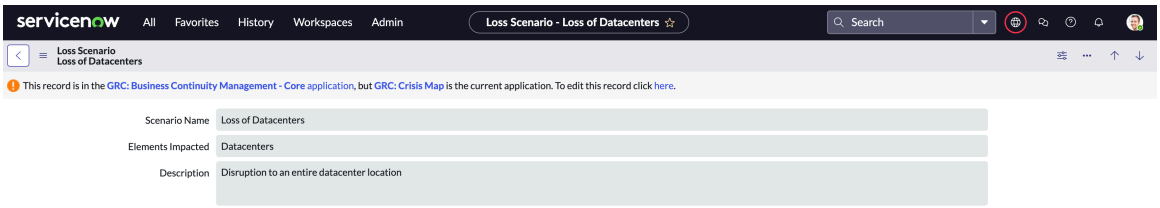
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. On the form, fill in the fields.

   For more information on the fields, see Loss Scenario record form.

   The following example shows the details of a loss scenario.




4. Select **Submit**.

### Loss Scenario record form

Use the Loss Scenario record form in BCM UIB Workspace to configure a plan for an identified loss scenario.

## Loss Scenario record form

For the description of the field values, see the following table.

**Loss Scenario record form**

| Field | Description |
|---|---|
| Scenario Name | Name of the impact scenario. |
| Elements impacted | Items or assets that are impacted because of the loss scenario. |
| Description | Short note about the loss scenario. |

### Configure an impact rating to assess the impact category

Configure an impact rating to assess an impact category as low, moderate, high, or critical. Use the **Impact Ratings** module in the Business Continuity Management application navigator to help you measure the intensity of the loss when a business downtime occurs.

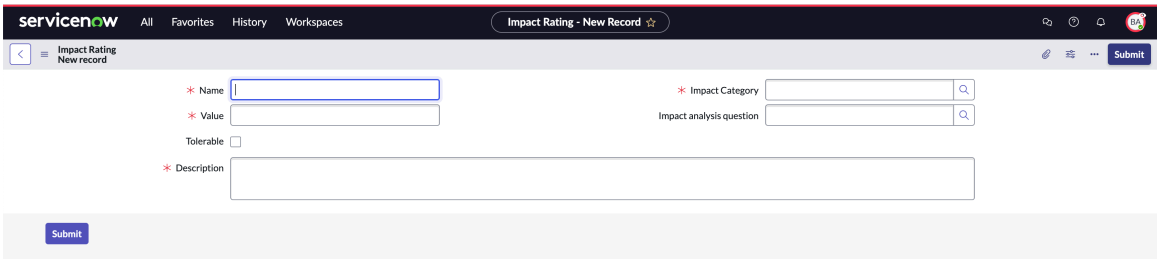
**Before you begin**
Role required: sn_bcm.admin

**Procedure**

1. Navigate to **Business Continuity** > **General Administration** > **Impact Ratings**.
2. Select **New**.

   The impact rating template is shown in the following example.

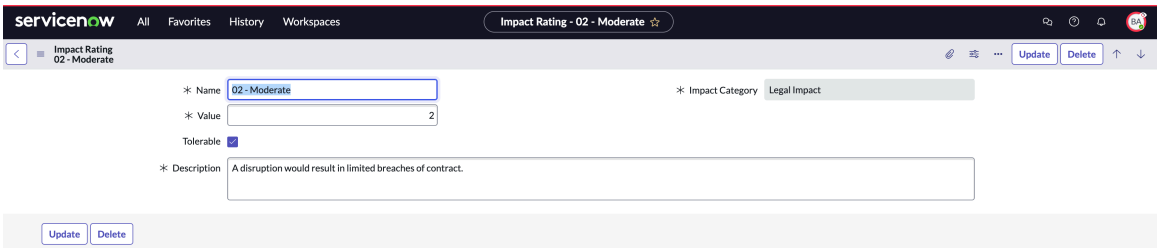
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. On the form, fill in the fields.

   For more information on the fields in the form, see Impact Rating record form.

   The following example shows an impact rating from the demo data.




4. Select **Submit**.

### Impact Rating record form

Use the Impact Rating record form to assess an impact category such as low, moderate, high, or critical by using BCM UIB Workspace.

## Impact Rating record form

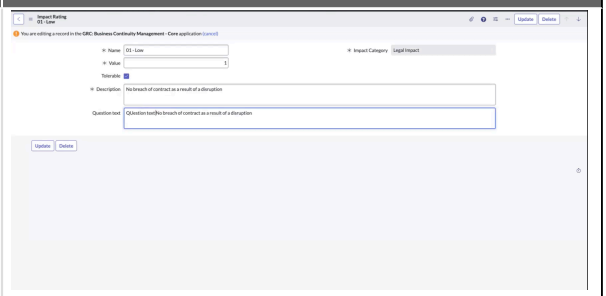
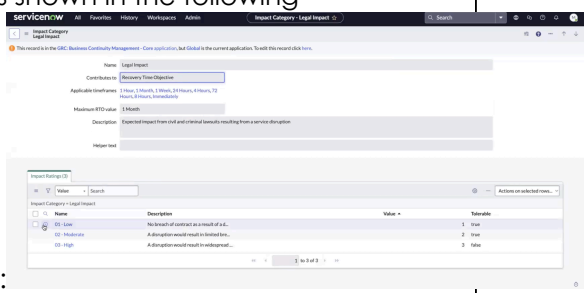
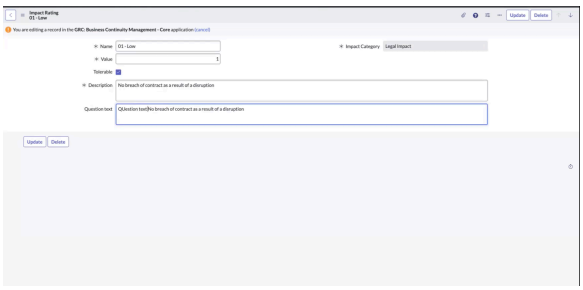
For a description of the field values, see the following table.

**Impact Rating record form**

| Field | Description |
|---|---|
| Name | Name of the impact rating. |
| Value | Numerical value for the impact rating. You can associate a unique numerical value to each impact rating. You cannot use the same value for any other impact rating in the BCM application.<br><br>For example, you can assign value *1* to the *01-Low* impact category as shown below. After you do so, you cannot assign value *1* to any other impact rating in your BCM application instance. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Impact Rating record form (continued)

| Field | Description |
|---|---|
| |  |
| Impact Category | Category of the impact. For example, Workforce impact, Regulatory impact, Revenue impact, and so on. |
| Impact analysis question | List of available impact analysis questions. This field is displayed if the impact category of the business disruption contributes to RPO. |
| Tolerable | Option for enabling the RTO impact as tolerable. This check box is displayed only if the impact category contributes to RTO. |
| Description | Short description about the impact rating. |
| Question text | Field to revise the question text. For the recovery time objective of an impact category, you can revise the question that is displayed in the RTO assessment questionnaire. You can navigate to the Impact Rating record as shown in the following example:  Update the question text for the RTO assessment as shown in the following example:  |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Impact Rating record form (continued)**

| Field | Description |
|---|---|
| | The revised question is then displayed in the RTO assessment of the business impact analysis record. |

### Configure a recovery tier for the business impact analysis

Configure a recovery tier with a set of business applications that follow a similar range of recovery time objective (RTO) values. Use the **Recovery Tiers** module in the Business Continuity Management application navigator to configure a recovery tier.

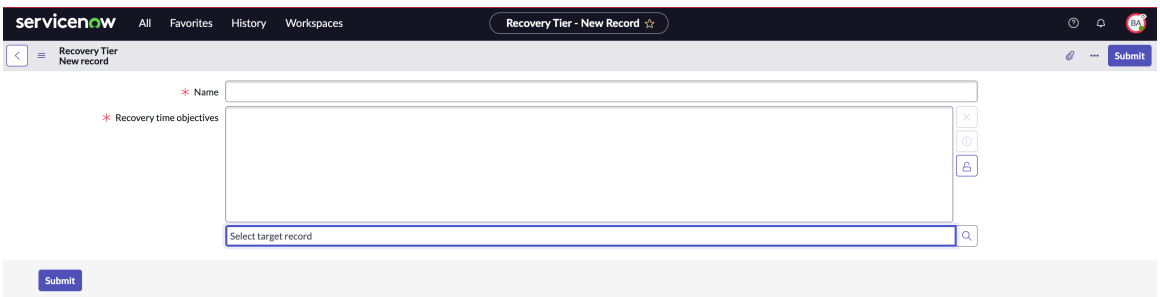
#### Before you begin

Role required: sn_bcm.admin

#### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Recovery Tiers**.
2. Select **New**.
3. On the form, fill in the fields.

   The recovery tier record is shown in the following example.




   For more information on the fields in the form, see Recovery Tier record form.

4. Select **Submit**.

### Recovery Tier record form

Use the Recovery Tier record form to configure a recovery tier with a set of business applications by using BCM UIB Workspace.

## Recovery Tier record form

For a description of the field values, see the following table.

**Recovery Tier record form**

| Field | Description |
|---|---|
| Name | Name for the recovery tier level. |
| Recovery time objectives | Metric that calculates how quickly the business should recover an element after a disaster. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Set up a recovery timeframe for a recovery tier

Set up a recovery timeframe for a recovery tier. The recovery timeframe starts from when a disruptive event happens to the time when your business can resume usual operations. You can use the **Recovery Timeframes** module in the Business Continuity Management application to set up the timeline for the recovery timeframe.

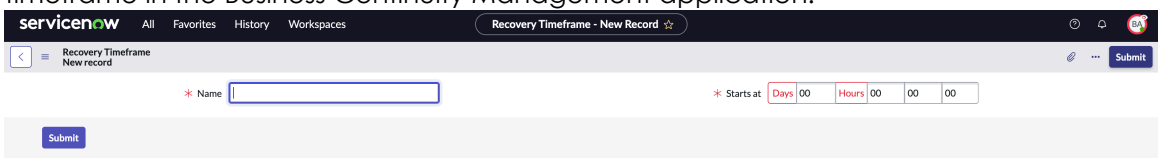
#### Before you begin

Role required: sn_bcm.admin

#### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Recovery Timeframes**.
2. Select **New**.
3. In the **Name** field, enter the name for the recovery timeframe.
4. In the **Starts at** field, enter the start of the timeline for the recovery timeframe in days, hours, minutes, seconds.

   The following example shows the configuration of a recovery timeframe in the Business Continuity Management application.




5. Select **Submit**.

### Configure a grid category for the grid configuration

Configure a grid category such as Dependency Assessment for the grid configuration. Use the **Grid Categories** module in the Business Continuity Management application navigator to configure the grid categories.

#### Before you begin

Role required: sn_bcm.admin

#### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Grid Categories**.
2. Select **New**.
3. On the form, fill in the fields.
   For more information on the fields in the form, see Grid category record form.
4. Select **Submit**.

### Grid category record form

Use the Grid category record form to configure a grid category such as Dependency Assessment for the grid configuration by using BCM UIB Workspace.

## Grid category record form

For a description of the field values, see the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Grid category record form

| Field | Description |
|---|---|
| Name | Name of the grid category. |
| Code | Code for the grid category. |
| Enable element context | Option to enable the element context for the grid category. |

### Configure the grid for the BIA dependency assessment

Configure the grid to render the BIA dependency assessment grid with configured columns. Use the **Grid Configurations** module in the Business Continuity Management application navigator to configure the grid.

#### Before you begin

Role required: sn_bcm.admin

#### Procedure

1. Navigate to **All** > **Business Continuity** > **General Administration** > **Grid Configurations**.
2. Select **New**.
3. On the form, fill in the fields.
   For more information, see Grid configuration record form.
4. Select **Submit**.

### Grid configuration record form

Use the Grid configuration record form to set up the BIA assessment grid in the classic Workspace.

## Grid configuration record form

For a description of the field values, see the following table.

### Grid configuration record form

| Field | Description |
|---|---|
| Name | Name of the grid configuration. |
| Grid category | Grid category for which the configuration is applicable. For example, DEP_ASSMNT. |
| Active | Option to set the record active. If the option is disabled, then the grid is rendered based on the configured view. Only one active configuration for a category and element should be present. |

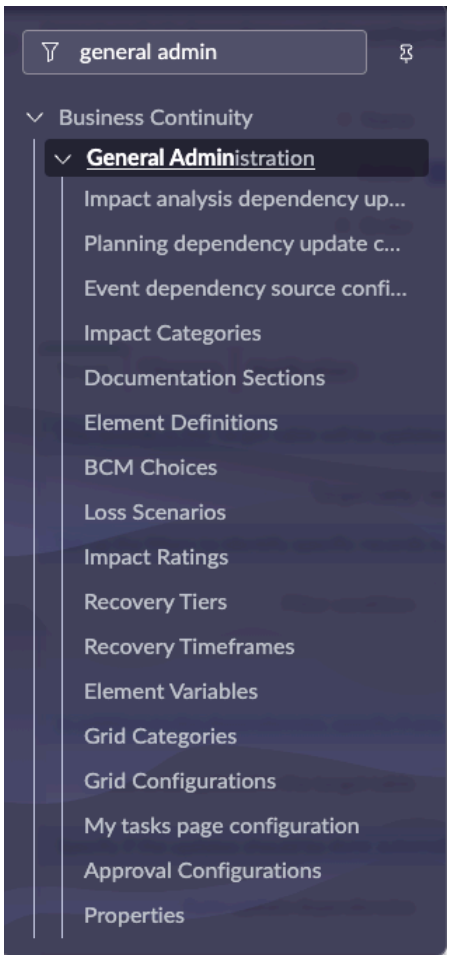
### My tasks page configurations

If you are the Business Continuity Management application user, you can use **My tasks page configurations** in the **General Administration** module to view your assigned tasks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

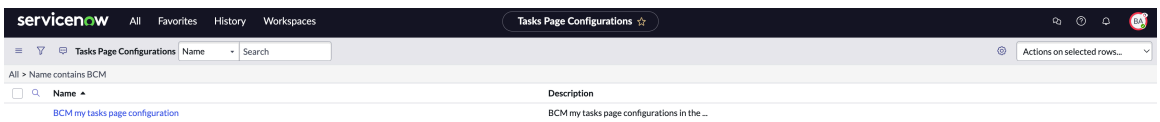
## My tasks page configurations module

The administrative tasks that are associated with the BCM application are listed in the **General Administration** module in the application UI. You can view My tasks page configurations in the **General Administration** module as shown in the following example.

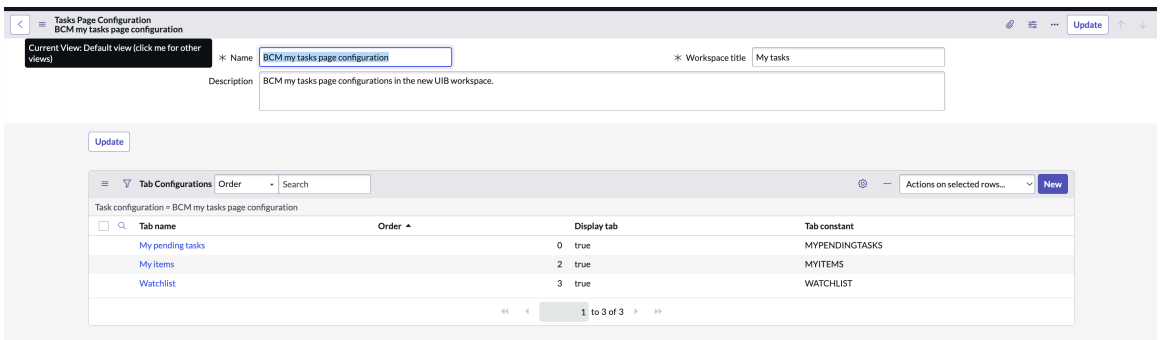



If you have the BCM administrator role, you can customize the BCM tasks in **My tasks page configuration**.

The **My tasks page configurations** module in the list view is shown in the following example.

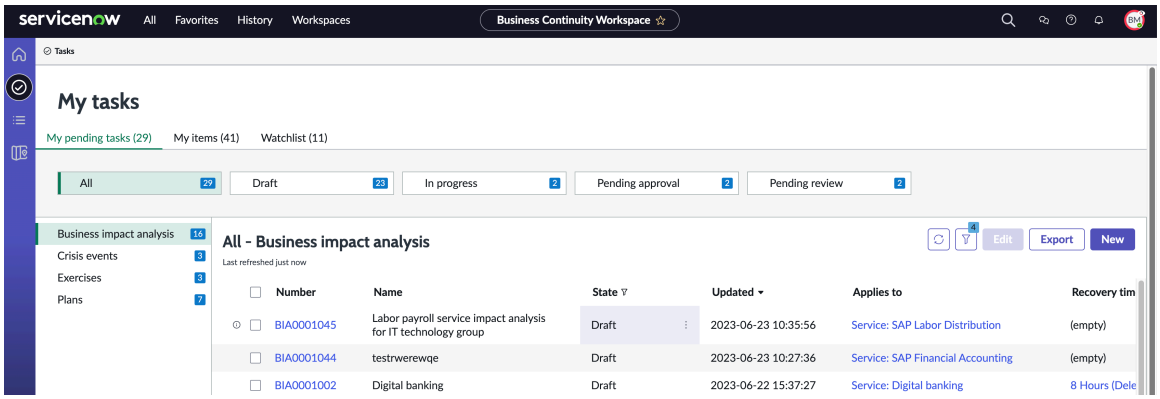



The **My tasks page configurations** module record is shown in the following example.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

My tasks page in the Home page displays the assigned tasks for the logged-in user as shown in the following example.




For more information on My tasks page view in BCM UIB Workspace, see My tasks page view.

### Approval configuration

Approver configurator provides you with capabilities to define multiple levels of approvals based on business rule definitions.

To set up multiple levels of approvals in your business impact analysis and business plans, you must configure the following setup steps:

- Set up approval configuration
- Set up approval levels
- Set up approval rules

**Note:**

For more information on the roles in the Business Continuity Management application, see Components installed with Business Continuity Management.

For more information on the roles in the GRC: Approver Configurator application, see Roles installed with GRC: Approver Configurator.

### Set up approval configuration

Set up approval configuration to enable multiple levels of approvals and select approvers for each level based on approval rules.

#### Before you begin

You must install GRC: Approver Configurator (sn_grc_appr) application for approval configurations.

Role required: sn_bcm.admin

**Note:** Granting this role to a user is equivalent to giving the user the admin role, because workflow script activities bypass access controls and grant access to all tables and database operations. Script activities do not bypass application scope settings.

#### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Approval Configurations**.
2. Click **New**.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Approval Configuration form

| Field | Description |
|---|---|
| Name | Name of the approval configuration. |
| Applies to | Table such as a business impact analysis, business continuity plan, events, or any table from which a record is submitted for approval. |
| Priority | Preference of approval configuration with higher priority. |
| Filter condition | Condition applied on the table with reference to the **Applies to** field.<br><br>The approval configuration with higher priority that matches the filter condition for the business document is selected for approver evaluation. |
| Active | Option to enable the approval configuration as active. |

**Note:** You cannot have more than one approval configuration applying to the table with the same priority.

4. Click **Submit**.

### Set up approval levels

Assign multiple levels of approvals to users or groups to support each step of your BIA, BCP, or events workflow processes.

#### Before you begin

Role required: sn_bcm.admin

**Note:** Granting this role to a user is equivalent to giving the user the admin role, because workflow script activities bypass access controls and grant access to all tables and database operations. Script activities do not bypass application scope settings.

#### Procedure

1. Navigate to **Business Continuity** > **General Administration** > **Approval Configurations**.
2. Click an approval configuration record in the list to set up the approval levels.
3. Click **New** in the Approval Levels section.
4. On the form, fill in the fields.

### Approval Level form

| Field | Description |
|---|---|
| Name | Name of the approval level. |
| Level | Stage of approval. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** You cannot have more than one approval level for an approval configuration with the same level.

5. Click **Submit**.

### Set up approval rules

Set up rules for approvals at each approval level by selecting an approver type and the requirement of approval from either one or all the stakeholders. Define filter conditions on the source table to which the approval rule is applied.

#### Before you begin
Role required: sn_bcm.admin

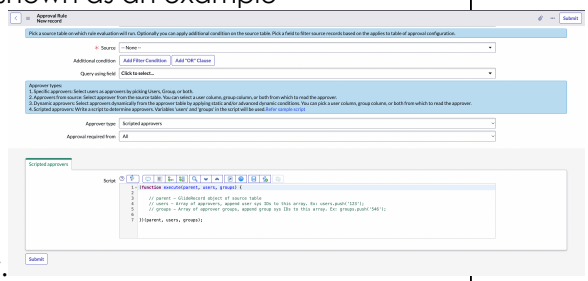
#### About this task
You can select specific approvers, approvers from the selected source table, dynamic approvers, or approvers that you choose to approve your business documents. The approvers can be a BIA owner, BCM lead, BCM manager, BCM admin, contributors, or one or all of them from the source table that you select.

#### Procedure
1. Navigate to **Business Continuity** > **General Administration** > **Approval Configurations**.
2. Click an approval configuration record in the list.
3. Click the approval levels record in the **Name** column of the Approval Levels section.
4. Click **New** in the Approval Rules section.
5. On the form, fill in the fields.

**Approval Rule form**

| Field | Description |
|---|---|
| Name | Name of the approval rule. |
| Source | Table to which the approval rule is applied. |
| Query using field | Field that connects the approving table and the source table. |
| Additional condition | Filter conditions applied on the source table. |
| Approver type | Type of approver.<br>◦ Specific approvers: Your choice of approvers.<br>◦ Approver from source: Users or groups from the source table.<br>◦ Dynamic approvers: Approvers selected dynamically from any table. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Scripted approvers: Script to determine approvers. See the script shown as an example below.<br>  <br>**Note:**<br>For security reasons, the BCM admin doesn't have write access to the **Script** field on the Approval Rule form. Only the Approver Configurator developer has create and write access to the **Script** field on the Approval Rule form.<br>If you have the BCM admin role, you can set up an approval rule only with the following types of approvers from the Approver type list:<br>◦ Specific approvers<br>◦ Approver from source<br>For more information on the roles in the GRC: Approver Configurator application, see Roles installed with GRC: Approver Configurator. |
| Approval required from | One or more stakeholders from whom the approval is required. |
| Description | Brief note about the approval rule. |
| Approvers | |
| Approvers from | Approver table.<br>This field is available only if the Approver type is **Approver from source** or **Dynamic approvers**. Defaults to the source table if it is Approver from source. |
| Filter by | Conditions to filter records from the approver table.<br>This field is available only if the Approver type is **Dynamic approvers**. |
| Advanced | Option to set a scripted dynamic condition. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| User field | User reference or list of approvers from the approver table. |
| Group field | User group reference as approver from the approver table. |
| Dynamic condition | Script field to apply advanced filter on approver table. |
| Users | One or more users designated as approvers. |
| Group | Group of approvers. |
| Scripted approvers | |
| Script | Script to determine approvers; **users** and **groups** in the script are selected as approvers. |

6. Click **Submit**.

## Example: Sample script to add assignees from CMDB dependencies as approvers

Field values on the form:

Name

Assignee of CMDB dependency as approvers.

Source

Dependency [sn_bia_dependency].

Query using field

Dependency Group.Impact Analysis

Approver type

Scripted approvers

### Sample script to add approvers

```
(function execute(parent, users, groups) {

    // parent - GlideRecord object of source table
    // users - List of approvers
    // groups - List of approver groups
    var gr = new GlideRecord('cmdb_ci');
    gr.addQuery('sys_id', parent.depends_on);
    gr.query();

    while (gr.next()) {
        users.push(gr.assigned_to.toString());
    }

})(parent, users, groups);
```

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### BCM properties

You can configure the BCM properties in the **Properties** module.

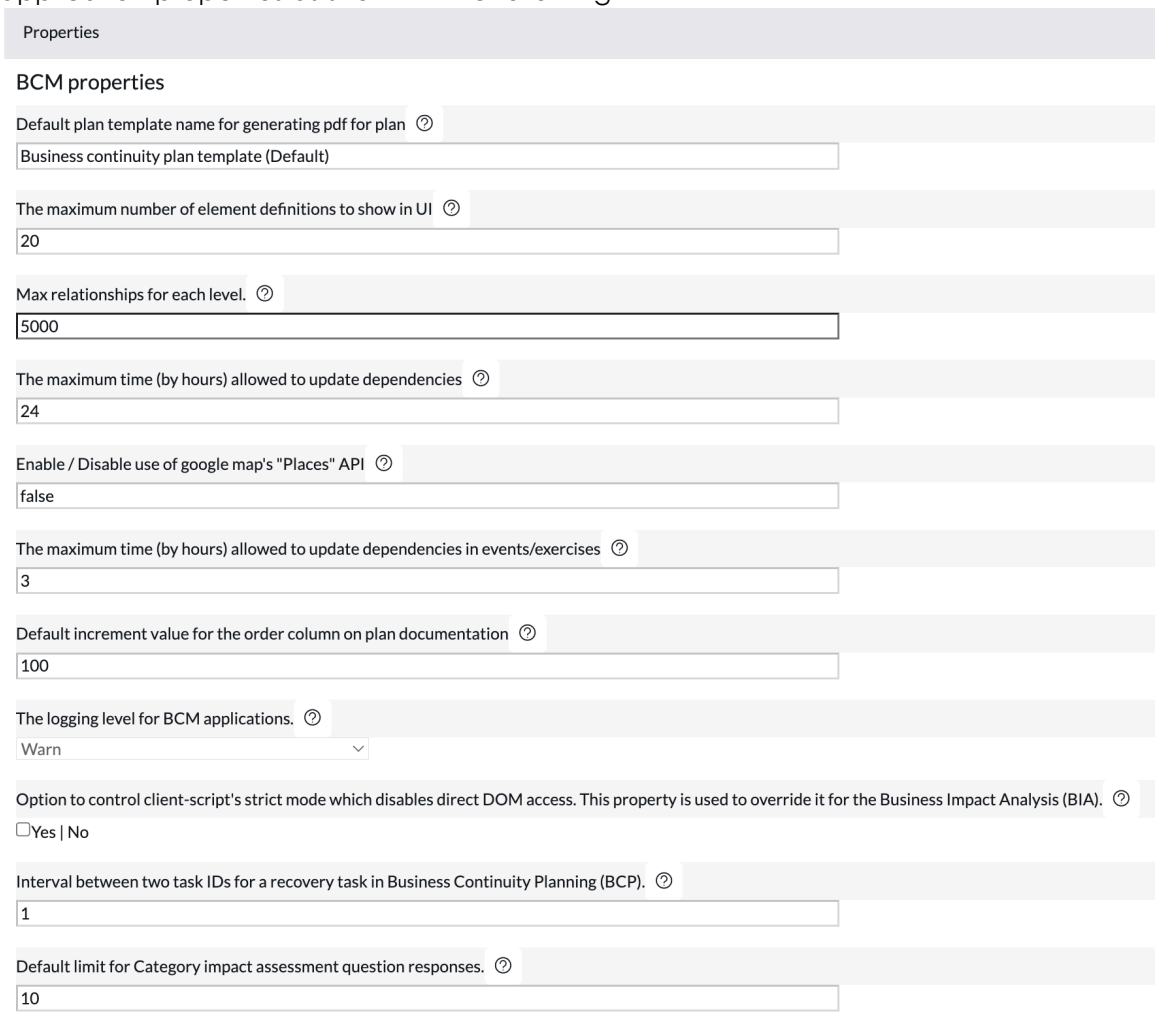
If you are the Business Continuity Management application user, you can view the properties for the Business Continuity Management application in **Properties** in the **General Administration** module.

You can view the **Properties** menu option in the **General Administration** module as shown in the following example.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can select the **Properties** module to view and configure the BCM application properties as shown in the following




example. Save

For more information on BCM properties, see Properties installed with Business Continuity Management.

### Properties installed with Business Continuity Management

Properties are added with the activation of Business Continuity Management.

#### BCM properties

| Sr. No | Name | Description |
|---|---|---|
| Scope: GRC: Business Continuity Planning | | |
| 1 | Default plan template name for generating the PDF for the plan<br><br>sn_bcp.default_pdf_plan_template | • **Type**: string<br>• **Default value**: Plan PDF Template Detailed<br>• **Location**: **Business Continuity** > **General Administration** > **Properties** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**BCM properties (continued)**

| Sr. No | Name | Description |
|---|---|---|
| 2 | Interval between two task IDs for a recovery task in Business Continuity Planning (BCP)<br><br>sn_bcp.taskIdOffset | • **Type**: numerical value<br>• **Default value**: 1<br>• **Location**: **Business Continuity** > **General Administration** > **Properties** |
| 3 | Default increment value for the order column on plan documentation<br><br>sn_bcp.document_order_increment | • **Type**: numerical value<br>• **Default value**: 100<br>• **Location**: **Business Continuity** > **General Administration** > **Properties** |
| Scope GRC: Business Impact Analysis | | |
| 4 | Option to control client-script's strict mode that disables direct DOM access. This property is used to override it for the Business Impact Analysis (BIA).<br><br>sn_bia.glide.script.block.client.globals | • **Type**: yes or no<br>• **Default value**: no<br>• **Location**: **Business Continuity** > **General Administration** > **Properties** |
| 5 | Max relationships for each level<br><br>sn_bia.cmdb_max_relationships_per_level | • **Type**: numerical value<br>• **Default value**: 5000<br>• **Location**: **Business Continuity** > **General Administration** > **Properties** |
| 6 | The maximum time (by hours) allowed to update dependencies (for BIA and BCP) | • **Type**: numerical value<br>• **Default value**:24<br>• **Location**: **Business Continuity** > **General Administration** > **Properties** |
| 7 | Default limit for Category impact assessment question responses | • **Type**: numerical value<br>• **Default value**: 10<br>• **Location**: **Business Continuity** > **General Administration** > **Properties** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**BCM properties (continued)**

| Sr. No | Name | Description |
|---|---|---|
| Scope: GRC: Business Continuity Management - Core | | |
| 8 | Logging level for BCM applications<br><br>sn_bcm.logging_verbosity | • **Type**: choice list (Debug, Info, Warn, Error)<br>• **Default value**: Warn<br>• **Location**: **Business Continuity** > **General Administration** > **Properties** |
| 9 | Maximum number of element definitions to show in UI<br><br>sn_bcm.element_definitions_limit | • **Type**: numerical value<br>• **Default value**:20<br>• **Location**: **Business Continuity** > **General Administration** > **Properties** |
| Scope: GRC: Crisis Map | | |
| 10 | Enable/Disable use of google map's "Places" API<br><br>sn_bcm_map.use_google_places_lib | • **Type**: true or false<br>• **Default value**: true<br>• **Location**: **Business Continuity** > **General Administration** > **Properties**<br><br>**Note:** Prior to enabling the Crisis Map feature, ensure that you have purchased and set up the Google Maps API. |
| 11 | The maximum time (by hours) allowed to update dependencies in events/ exercises | • **Type**: numerical value<br>• **Default value**: 3<br>• **Location**: **Business Continuity** > **General Administration** > **Properties** |

## Setup for a business impact analysis

The administrative tasks that are associated with a business impact analysis are listed in the **General Administration** module in the Business Continuity Management application. The BIA administrator with the sn_bia.bia_admin role is responsible to perform the administrative tasks that are associated with a business impact analysis.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Typically, the BIA administrator with the sn_bia.bia_admin role configures the BIA templates. For more information, see Configure a business impact analysis (BIA) template.

### Configure a business impact analysis (BIA) template

Configure a business impact analysis (BIA) template to configure a business impact analysis with the standard object types. Use the **BIA Templates** module in the Business Continuity Management application navigator and select the type of the elements, impact categories, and dependencies that are assessed by using the BIA template.

#### Before you begin

Role required: sn_bcm.admin

#### Procedure

1. Navigate to **All** > **Business Continuity** > **BIA Configuration** > **BIA Templates**.
2. Select **New**.
3. On the form, fill in the fields.
   For more information on the fields in the form, see BIA Template record form.
4. Select **Submit**.

### BIA Template record form

Use the BIA Template record form to add details about the new business impact analysis such as name, description, elements, impact categories, and so on in BCM UIB Workspace.

## BIA Template record form

For a description of the field values, see the following table.

**BIA Template record form**

| Field | Description |
|---|---|
| Name | Name of the BIA template. |
| Description | Brief description about the template. |
| Primary Element Assessed | Primary object type or an element that is being assessed for which the template is used. |
| Impact Categories | Category of impact that is relevant to an organization and that is assessed during the business impact analysis. It can be revenue, legal, regulatory, reputation impact, and so on. |
| Dependency Assessments | Category of items or assets that the business function depends on such as locations or business applications. The dependencies are identified and assessed as part of the business impact analysis. |
| Include CIA | Option to include Confidentiality, Integrity, and Availability to BIA. If the primary element that is being analysed has critical data and whether it must include Confidentiality, |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**BIA Template record form (continued)**

| Field | Description |
|---|---|
| | Integrity and Availability information in the analysis, set the flag as **Yes**.<br><br>The field appears only if the elements that selected for the **Primary Element Assessed** field in the same form require data backup. |

## Setup for a business continuity plan

The BCP administrator can perform certain administrative tasks that are listed in the **General Administration** section of the Business Continuity Management application.

The administrative tasks for business continuity planning are listed in the **General Administration** section in the application navigator.

Typically, the BCP plan administrator with the sn_bcp.plan_admin role performs the following administrative tasks:

- Configure plan templates: For more information, see Configure a business continuity plan template for your business.
- Configure documentation sections in the business continuity plan: For more information, see Configure the documentation section for a business continuity plan.
- Configure loss scenarios in the business continuity plan: For more information, see Configure a loss scenario in your business continuity plan.

### Configuring the plan template for the business continuity plan

As a BCP plan manager, you can create a business continuity plan that can be used for your respective business units during a disruptive event. The Business Continuity Management application provides pre-configured business continuity plan templates. You can streamline the process of a plan creation by using pre-configured plan templates. You can also create a plan template for your business requirement.

You can view the pre-configured plan templates for business continuity planning in the **General Administration** section in the application navigator.

Using a plan template gives you a standard plan layout that has the document sections, loss scenarios, and primary elements that are to be recovered. Plan templates help you to focus on the plan content, its tasks, and the effective implementation of the plan.

Creating a plan helps an organization to identify processes, locations, and assets that must be recovered as a priority when there is a disruption. Selecting a plan type helps to identify the elements for recovery and the time by which it should be done.

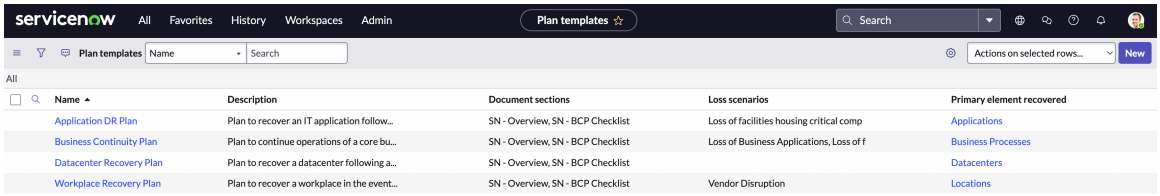
## Using business continuity plan templates

The Business Continuity Management application provides the following business continuity plan templates that are installed with demo data:

- **Application DR Plan**
- **Business Continuity Plan**
- **Datacenter Recovery Plan**
- **Workplace Recovery Plan**

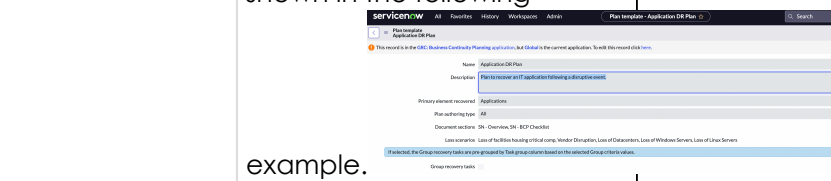
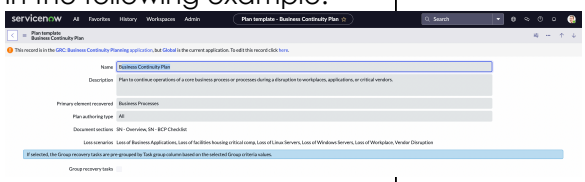
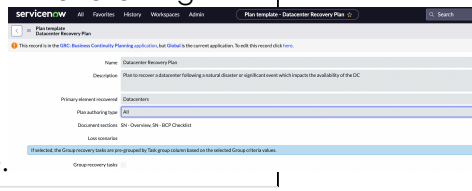
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The business continuity plan templates that are installed with demo data are shown in the following example.



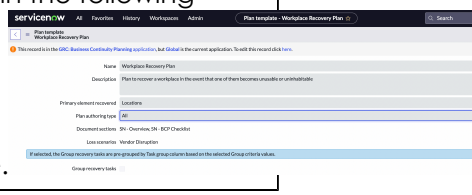

See the following table for more information on different types of demo data plan templates that you can use in the Business Continuity Management application.

### Demo data plan templates

| Name | Primary element recovered | Description |
|---|---|---|
| Application DR Plan | Applications | Plan to recover an IT application following a disruptive event. A sample Application DR Plan template is shown in the following example.  |
| Business Continuity Plan | Business Processes | Plan to continue operations of a core business process or processes during a disruption to workplaces, applications, or critical vendors. A sample Business Continuity Plan template is shown in the following example.  |
| Datacenter Recovery Plan | Datacenters | Plan to recover a datacenter following a natural disaster or significant event that impacts the availability of a datacenter. A sample Datacenter Recovery Plan template is shown in the following example.  |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Demo data plan templates (continued)**

| Name | Primary element recovered | Description |
|---|---|---|
| Workplace Recovery Plan | Locations | Plan to recover a workplace in the event that one of them becomes unusable or uninhabitable. A sample Workplace Recovery Plan template is shown in the following example.  |

## Creating a plan template for your business requirement

Instead of using the demo data templates, you can create a template for your specific requirement. For more information on creating a plan template for your business requirement, see Configure a business continuity plan template for your business.

### Configure a business continuity plan template for your business

Configure a business continuity plan template in the Business Continuity Management application for your business. You can use the plan template to recover a specific primary element such as Employees or Web Servers. Similarly, you can create a plan template for different plan authoring types such as documentation, loss scenarios, and recovery tasks.

#### Before you begin

Role required: sn_bcm.admin

#### About this task

The sn_bcm.admin role contains the sn_bcp.plan_admin role. The sn_bcm.admin role is necessary to view the **Plan Templates** menu. The BCM administrator can navigate to the **Plan Templates** menu and then the plan administrator can update the plan templates.

By configuring the plan template, you can:

- Define the primary object type that has to be recovered.
- Define documentation sections that should be included right at the beginning of a plan.
- Identify the loss scenarios and plan accordingly using the template.

#### Procedure

1. Navigate to **Business Continuity** > **Plan Configuration** > **Plan Templates**.
2. Select **New**.
3. On the Plan Template form, fill in the fields.
   For more information on the fields, see Plan Template form.
4. Select **Submit**.

### Plan Template form

Use the Plan Template form in BCM UIB Workspace to add details about the business continuity plan.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Plan Template form

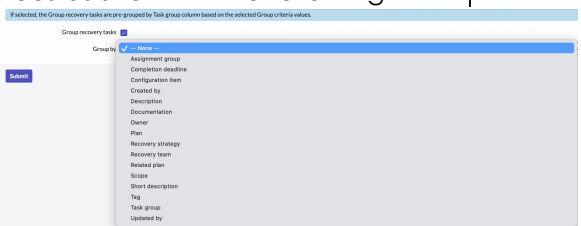
For the description of the field values, see the following table.

**Plan Template form**

| Field | Description |
|---|---|
| Name | Name of the plan template. |
| Description | Brief description about the plan template. |
| Primary Element Recovered | Primary object type or an element identified to be recovered in the plan. |
| Plan authoring type | Different phases or sections of a plan that are available as options when you create a continuity plan using this template. These options show as tabs in the BCP workspace as you proceed to complete the plan details.<br>• **All** (Default): All options like Documentation, Loss Scenarios, Recovery tasks, and Recovery teams are displayed in the plan that uses this template. You can view these options as tabs in the workspace.<br>• **Documentation**: Plan that uses this template displays the documentation option along with selected dependencies. Documentation tab along with Recovery tasks and Recovery teams are available for view in the workspace.<br>• **Loss Scenarios**: Displays the loss scenarios along with Recovery tasks, Recovery teams, and other selected dependencies in the plan that uses this template.<br>• **Recovery tasks**: Displays recovery tasks and Recovery teams associated to the plan type that uses this template. |
| Document sections | Documentation sections to be added to the plan. Available options are:<br>• BCP-Assumtions<br>• BCP-Objectives<br>• BCP-Scope<br>• BIA-Overview<br>• SN-BCP Checklist<br>• SN-Overview |
| Loss scenarios | Loss scenarios to be added to the plan. Available options are: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Plan Template form (continued)**

| Field | Description |
|---|---|
| | • Loss of facilities housing critical comp<br>• Loss of Linux Servers<br>• Loss of Datacenters<br>• Loss of Workplace<br>• Loss of Business Applications<br>• Loss of Personnel<br>• Vendor Disruption<br>• Loss of Windows Servers<br><br>You can also create a loss scenario and add it to the template. For more information on creating a loss scenario, see . |
| Group recovery tasks | Option to group the recovery tasks. If this option is selected, the Group recovery tasks are pre-grouped by the **Task group** column, based on the selected **Group by** criteria values as shown in the following example.  |

## Format the PDF templates for BIA, BCP, and Events

Format the PDF templates that are used in generating the PDF of a business impact analysis, business continuity plan, or event. You can format the PDF according to your organizational requirements and templates.

### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, sn_bcm.planner

Ensure that you have downloaded the PDF of a business impact analysis, business continuity plan, or event according to the steps mentioned in the following topics:

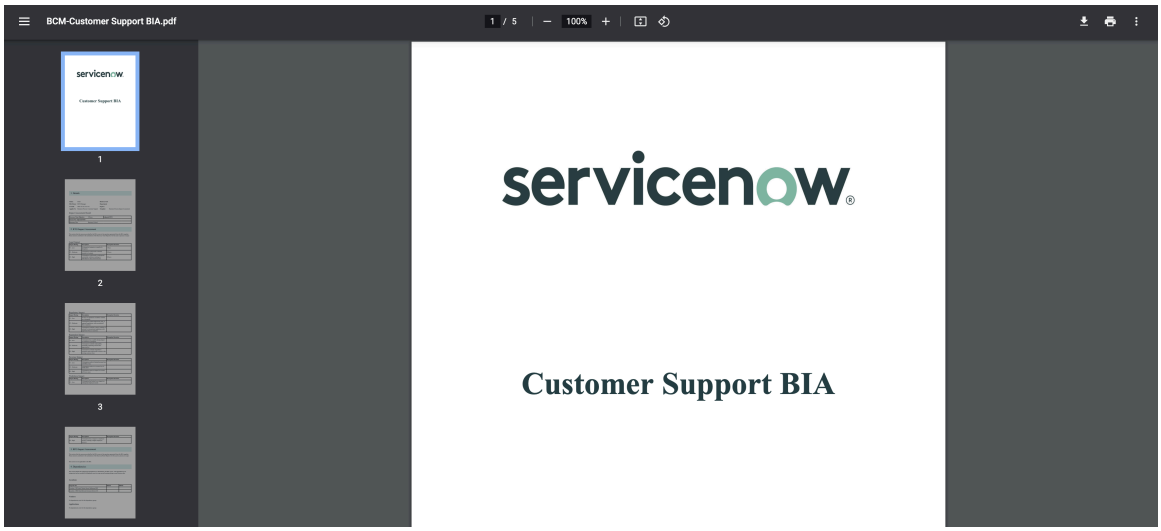
- Generate the PDF of a business impact analysis
- Generate the PDF of a business continuity plan
- Generate the PDF of an exercise or crisis event

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Business Impact Analysis** record and open the PDF that is saved on the **Details** tab.
3. Update the title of the PDF and the fonts according to your organizational templates.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following example shows the PDF that can be updated according to your requirements.




You can use the same process to update the PDF of a business impact analysis, business continuity plan, exercise, or crisis event.

**Note:**

As an administrator, you can navigate to **All Document Templates** in an instance to view the document templates that are provided with the BCM application.

You can also use an editable and fillable PDF template to format the PDF. For more information on the PDF document template that can be used to customize your PDFs, see Configure a PDF document template.

4. Save the PDF.
   You can save the PDF for a future reference.

## Configure 360° relationship registries and views

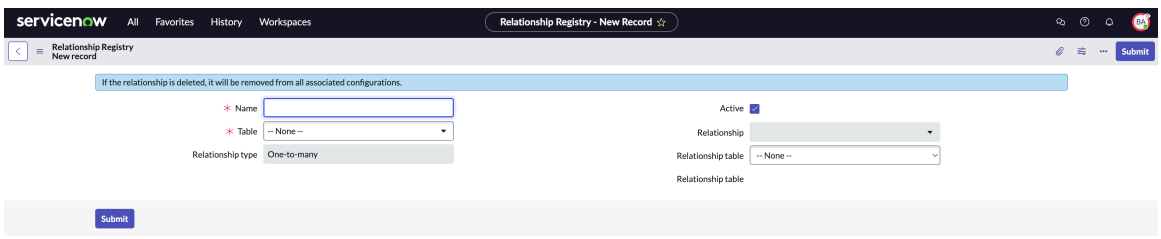
Configure 360° view configurations with the sn_bcm.admin role.

### Before you begin

Role required: sn_bcm.admin

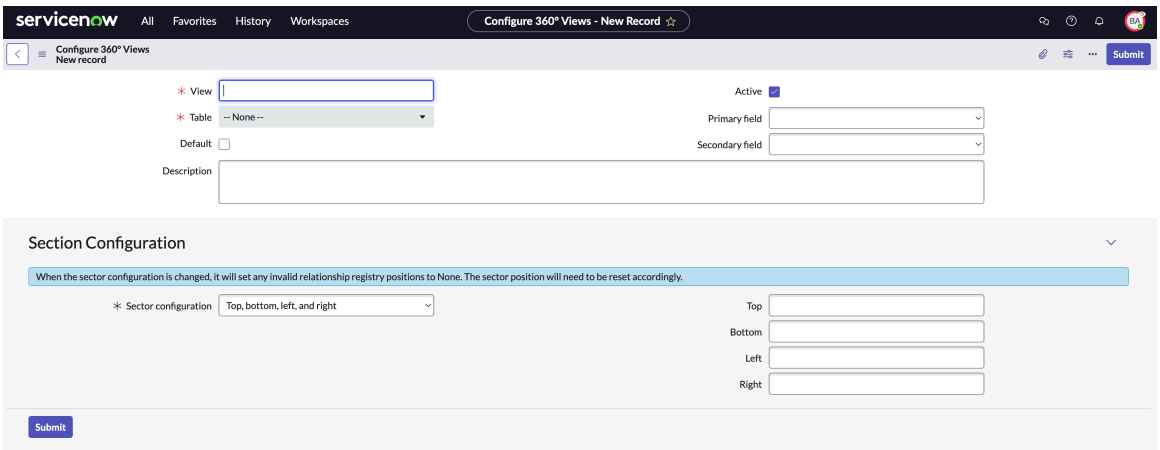
### Procedure

1. Navigate to **All** > **360° View Configurations** > **Configure 360° Views**.
2. To configure the relationships for the records, navigate to **360° View Configurations** > **Relationship Registries**.
   The form is shown in the following example.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select **Update**.
4. To configure 360° views for the records, navigate to **360° View Configurations** > **Configure 360° Views**.
   The form is shown in the following example.




5. Select **Update**.
   For more information on 360° configurations, see Configure 360° views.

## Setup for Everbridge notifications

The setup steps help you to establish a consistent connection and successful notification delivery workflow with Everbridge notifications system. The BCM administrators and application users must configure certain pre-requisite data so that you can set up emergency notifications in BCM UIB Workspace.

The following pre-requisite configurations are required to be set up for sending an emergency notification and monitoring the notification workflow:

- To create a connection and authenticate your credentials with Everbridge, see Create a connection and authenticate the credential with Everbridge.
- To get the delivery details of the contacts from Everbridge and use them to send a notification, see Import the delivery channels from Everbridge.
- To get the details about the type of contacts from Everbridge, see Import the record types from Everbridge.
- To pre-configure a notification template to send an email or SMS to your contacts, see Create a template for an emergency notification.
- To create contacts for sending the notification, see Create the contacts for an emergency notification.
- To set up rules in filtering the contacts from the user table, see Create the contact import rules.
- To create a group of contacts, see Create a notification contact group.

Here is a flow diagram that shows how the different setup steps are connected for the integration:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Setup flow for an emergency notification




### Create a connection and authenticate the credential with Everbridge

Establish a connection and authenticate your login credentials with an Everbridge instance. You can then send out a notification using the delivery channel. This connection helps you to send and receive communications with an Everbridge instance.

#### Before you begin

Role required: sn_bcm.admin

#### Procedure

1. Navigate to **Business Continuity** > **Everbridge Notification Configuration** > **Connection & Credential Alias**.
2. Select the **Create New Connection & Credential** related link.
3. On the form, fill in the fields.
   For more information on the fields, see Create Connection and Credential form.
4. Select **Create**.
   A connection is established to send and receive communications with an Everbridge instance.

### Create Connection and Credential form

Use the Create Connection and Credential form to establish a connection and authenticate your login credentials with an Everbridge instance.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Create Connection and Credential form

### Create Connection and Credential form

| Field | Description |
|---|---|
| Connection Name | Name of the connection. Enter **Everbridge** Connection. |
| Connection URL | Everbridge API base address. |
| Organization ID | Organization ID of Everbridge.<br>**Note:** You can get the organization ID from the Everbridge instance. |
| Incident Template ID | Unique ID of the Everbridge incident template.<br>**Note:** You can get the ID from the Everbridge instance. |
| Credential Name | Name of the Everbridge credential. |
| Username | User name of the API user in Everbridge. |
| Password | Password to validate and establish the connection. |

### Import the delivery channels from Everbridge

Import the delivery channels from the Everbridge instance. You can then easily send the notifications through the delivery channels.

#### Before you begin
Role required: sn_bcm.admin

#### About this task
You may face challenges in connecting with your stakeholders at the time of a crisis. Your notifications may not reach the stakeholders as they may no longer use the same delivery methods. When you have imported the delivery channels to reach your contacts and selected groups, you can send the notifications in an easier and manageable way.

#### Procedure
1. Navigate to **Business Continuity** > **Everbridge Notification Configuration** > **Delivery Channels**.
2. Select **Import**.
   All delivery channels are imported from the Everbridge instance successfully. When the notification is successful, you receive a message of confirmation from Everbridge.

### Import the record types from Everbridge

Import the record types for your organization ID from Everbridge and use them to create the contacts for notifications.

#### Before you begin
Role required: sn_bcm.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task
Record types are information stored in Everbridge that are required to create the contacts for notifications.

### Procedure
1. Navigate to **Business Continuity** > **Everbridge notification Configuration** > **Record Types**.
2. Select **Import**.
   Record types for your organization ID with the category are imported from the Everbridge instance. If the record type is not imported, you may receive an error message.

#### Create a template for an emergency notification

Create a template with pre-defined information. You can then use it to send the notifications to your users in an emergency.

### Before you begin
Role required: sn_bcm.admin

### About this task
You can define a sample template with the draft of an email. It can contain the notification format for a particular emergency crisis that might affect a specific business location or facility.

### Procedure
1. Navigate to **Business Continuity** > **Everbridge Notification Configuration** > **Notification Templates**.
2. Select **New**.
3. On the form, fill in the fields.
   For more information on the fields, see Notification Template form.
4. Select **Submit**.

#### Notification Template form

Use the Notification Template form to create a template with pre-defined information for sending out the notifications.

## Notification Template form

**Notification Template form**

| Field | Description |
|---|---|
| Name | Name of the notification template. |
| Description | Short note about the purpose of the template. |
| Delivery channels | Communication channels that are used for sending the notification. |
| Subject | Title of the notification. |
| Message body | Introductory text message for the notification. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Notification Template form (continued)**

| Field | Description |
|---|---|
| Foot note | Closing message or a foot note for the notification. |
| SMS text | Text message sent through SMS. |

## Create the contacts for an emergency notification

Create the contacts manually to send out an emergency notification and synchronize them with the Everbridge instance.

### Before you begin

Role required: sn_bcm.admin

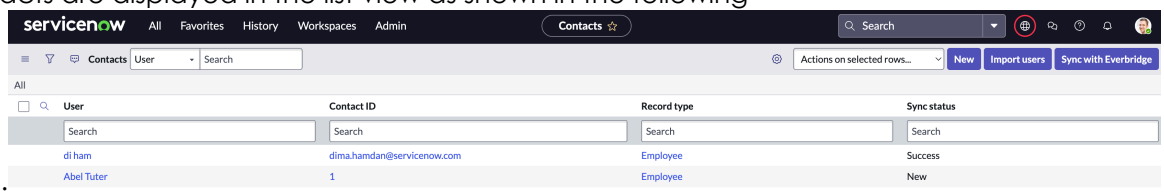
### About this task

After creating the contacts from the user list, you can update and synchronize them with the Everbridge instance.

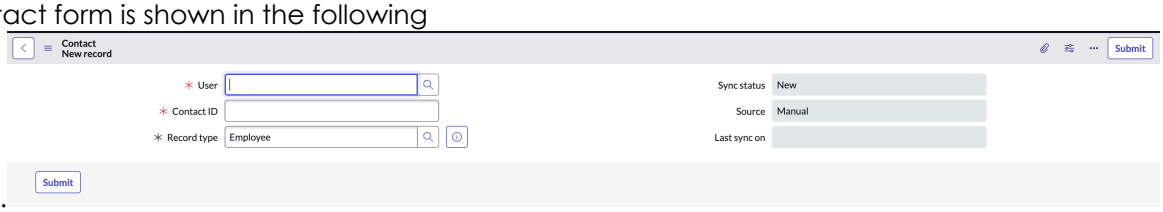
Delivery channels are imported from the Everbridge instance to the delivery channels table. By using the imported delivery channels, you can manually create the contact delivery details.

### Procedure

1. Navigate to **Business Continuity** > **Everbridge Contact Configuration** > **Contacts**.
   The contacts are displayed in the list view as shown in the following example.




2. Select **New**.
   The Contact form is shown in the following example.




3. On the form, fill in the fields.

   You can delete a contact that you created manually from the User table. However, the contact must be in **New** state. If the referenced user record is deleted, then a scheduled job that runs weekly deletes the contact from the Contacts table.

   For more information on the fields, see Contact form.

4. Select **Submit**.

5. To import contacts based on contact sync rules, select the **Import users** button.
   To import the contacts using a sync rule, you must first Create the contact import rules.
   Refresh the form page to get the imported list of users.

   **Import users** action reads the Users table [sys_user] based on the contact sync rules and creates a record in the Contacts table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. To synchronize your list of contacts with that of Everbridge, select the **Sync with Everbridge** button.
   After the contacts are synchronized with Everbridge, the status of the sync action is recorded in the **Sync status** field. The unique ID of the contacts that are synced successfully in Everbridge are recorded as the **External contact ID** of the Contacts table.

### Contact form

Use the Contact form to create the contacts manually and then synchronize the contacts with Everbridge.

## Contact form

### Contact form

| Field | Description |
|---|---|
| Source | Source of the contacts.<br>• If you created the contacts manually from the users' list, then the source is **Manual**.<br>• If you had used the sync rule to create the contacts, then the source is **Sync rule**. |
| Last sync on | Date on which the contact was last synchronized with Everbridge. |
| Contact ID | Unique ID of the contact. |
| Sync status | Sync status when the contact is created. Defaults to **New** when the contact is created. The status can also be:<br>• **Success**: When the contact is successfully synced with Everbridge<br>• **Error**: If there is an error in syncing<br>• **Updated**: If the contact or the delivery details were modified |
| User | User reference from the Users table [sys_user]. |
| External contact ID | Contact ID in Everbridge. |
| Sync error | Error in syncing the contact with Everbridge. |

### Create the contact import rules

Create a contact import rule to apply on the User table. You can then filter out the users as the contacts for emergency notifications.

**Before you begin**
Role required: sn_bcm.admin

**About this task**
The default table on which the contact import rule is applied is the User table [sys_user]. The sys_id of the user table and the unique contact ID of the Contacts table are mapped.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **Business Continuity** > **Everbridge Contact Configuration** > **Contact Import Rules**.
2. Select **New**.
3. On the form, fill in the fields.
   For more information, see Contact Import Rules form.
4. Select **Submit**.

#### Contact Import Rules form

Use the Contact Import Rules form to create a contact import rule that you can apply on the User table.

**Contact Import Rules form**

| Field | Description |
|---|---|
| Name | Name of the import rule. |
| Table | User table [sys_user] for the rule. |
| Filter condition | Condition applied on the User table to filter the records. |
| Record type | Default category of the record type. |
| User mapping | Unique user reference from the Users table. |
| Contact ID mapping | Unique ID of each contact that is used to sync with Everbridge. |

#### Create a notification contact group

Create a notification contact group using the Now Platform groups. Use the group members as the contacts for an emergency notification. Synchronize the group members as the contacts with Everbridge and track the non-synchronized members as exceptions.

### Before you begin

Role required: sn_bcm.admin

### Procedure

1. Navigate to **Business Continuity** > **Everbridge Contact Configuration** > **Notification Contact Groups**.
2. Select **New**.
3. On the form, fill in the fields.
   For more information, see Notification Contact Group form.
4. Select **Submit**.
5. To synchronize the group with the groups in Everbridge, select **Sync Groups to Everbridge**.
   Refresh the page to get the synchronized status of the group.

   If a group is not synchronized with Everbridge, then you get an error message.
6. To view the names of the group members that did not synchronize with Everbridge, select the **Group User Exceptions** related list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Example:**
There are five members in a group, out of which four members are already synced with Everbridge and existing as contacts. When you synchronize the group, a group is created in Everbridge with the four synced group members. However, the unsynchronized single member is logged as an exception displaying a message as to why the syncing failed.

You can synchronize this particular contact first and then the group with Everbridge.

#### Notification Contact Group form

Use the Notification Contact Group form to create a notification contact group.

## Notification Contact Group form

**Notification Contact Group form**

| Field | Description |
|---|---|
| Group | Reference to the User Group table. |
| Sync status | Sync status for the group. Defaults to **New** when the group is created.<br>• **Success**: The contact group is successfully synchronized with Everbridge.<br>• **Error**: If there is an error in syncing<br>• **Updated**: If the contact group is modified |
| Last sync on | Date on which the group was last synchronized with Everbridge. |

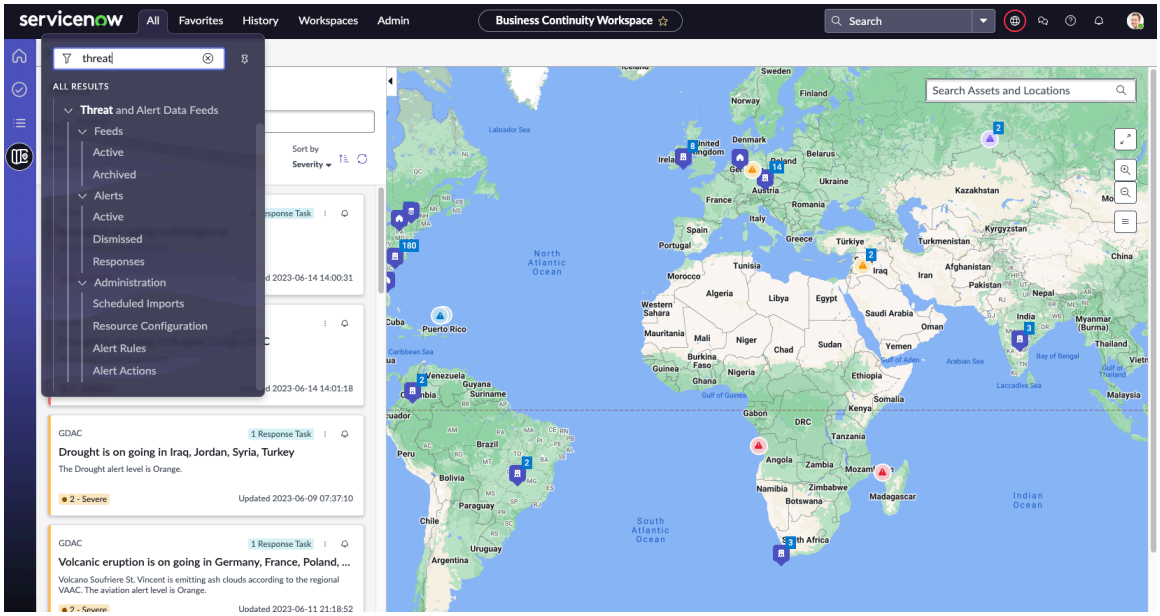
## Setup for Crisis map

The BCM administrator can perform the administrative tasks to set up the Crisis map interface.

The BCM administrator performs the administrative tasks to set up the threat alerts and data feeds in Crisis map. The administrative tasks are displayed under **Administration** in the **Threat and Alert Data Feeds** module as shown in the following example.

**Note:** Prior to enabling the Crisis Map feature, ensure that you have purchased and set up Google Maps API.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




If you have the BCM administrator role, perform the following administrative tasks to set up the Crisis map:

- **Scheduled Imports**: Configure a Scheduled Data Imports record for the Crisis map application. For more information, see Configure a Scheduled Data Imports record.
- **Resource Configuration**: Configure a Resource Configuration record for the Crisis map application. For more information, see Configure a Resource Configuration record for Crisis map.
- **Alert Rules**: Configure an alert rule in Crisis map so that you can specify the conditions under which a feed can be displayed in the dashboard as an alert. For more information, see Configure an alert rule in Crisis map.
- **Alert Actions**: Configure an alert action in UIB Workspace for the Crisis map application. For more information, see Configure an alert action in Crisis map.

### Configure a Scheduled Data Imports record

Configure a Scheduled Data Imports record for the Crisis map application. You can then manage your subscriptions to the threat feeds from an internal or external source in UIB Workspace.

#### Before you begin

Role required: admin

You must set up the Google maps for enabling the crisis map functionality. For more information, see Set up Google Maps API.

#### About this task

Threat feeds provide a situational awareness of potential or current threats to the security of your organization. Threat alerts can be weather alerts, pandemic alerts, geopolitical situations, or internal events like security incidents and system outages.

#### Procedure

1. Navigate to **Threat and Alert Data Feeds** > **Administration** > **Scheduled Imports**.
   Following two scheduled data imports exist within the base system.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Name | Data source |
|---|---|
| GDAC Feed Source | GDAC Feeds |
| Weather.gov Severe Alerts Scheduled Import | Weather Gov Alerts |

2. To add a new scheduled data import record, select **New**.
3. On the form, fill in the fields.
   For more information on the Scheduled Data Imports form, see Scheduled Data Imports form.
4. Select **Submit**.

**Result**
The data import record is displayed in the **Scheduled Data Imports** record page.

### Scheduled Data Imports form

Use the Scheduled Data Imports form in BCM UIB Workspace to add details about a Scheduled data imports record.

#### Scheduled Data Imports form

| Field | Description |
|---|---|
| Name | Name of the scheduled import. Normally the source is the name. |
| Data source | Internal or external source of the threat and alert data used for import. |
| Run as | User who has the permission to import the threat alerts. |
| Active | Option for enabling the alert as active. |
| Application | Read-only field. The field helps distinguish items relevant to the Crisis map. |
| Run | Frequency at which the data is imported. |
| Time | Time in Hours, Minutes, Seconds for the data import. |
| Conditional | Option to indicate if a conditional script is required for the threat alert import. |
| Concurrent Import | Option for enabling concurrent imports. |
| Execute pre-import script | Option for enabling the execution of a pre-import script. |
| Execute post-import script | Option for enabling the execution of a post-import script. |

### Configure a Resource Configuration record for Crisis map

Configure a Resource Configuration record for the Crisis map application in UIB Workspace. You can then plot the assets of your organization on the Crisis map. The assets can be

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

locations, employees, datacenters, suppliers, and others. Configuring resources is also required as an input to set up the alert rules.

### Before you begin
Role required: sn_bcm.program_manager

Set up the Google maps for enabling the Crisis map functionality. For more information, see Set up Google Maps API.

### Procedure
1. Navigate to **Threat and Alert Data Feeds** > **Administration** > **Resource Configurations**.
2. To add a new resource configuration record, select **New**.
3. On the form, fill in the fields.
   For more information on the Resource Configuration form, see Resource Configuration form.
4. Select **Submit**.

### Result
The resource is displayed in the **Resource Configurations** record page.

#### Resource Configuration form
Use the Resource Configuration form in BCM UIB Workspace to add details about a resource configuration record.

**Resource Configuration form**

| Field | Description |
|---|---|
| Name | Name of the resource configuration used in the map visualization. |
| Icon | Image representing a resource item on the map. |
| Table | Table for resources to plot on the map. |
| Location field | Location column of the table used as location on the map. |
| Use Coordinates | Option for enabling coordinates to plot the resources on the geo-map. |
| Application | Read-only field. The field helps distinguish items relevant to the Crisis map. |
| Active | Option to indicate that the resource configuration is active. |
| Order | Order of the record. |
| Category | Category of the record. The value is **BCM**. It helps to identify the BCM-related resources when multiple applications use the component. |
| Searchable | Option to indicate if the resource is searchable in the map visualization. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Resource Configuration form (continued)**

| Field | Description |
|---|---|
| Contact User Field | Contact for communication for the resource in focus. |
| Contact Alias | Contacts for identification. |
| Display Fields | Fields selected for display as the contacts. |
| Conditions | Conditions for filtering records from the table. |

### Configure an alert rule in Crisis map

Configure an alert rule in Crisis map so that you can specify the conditions under which a feed can be displayed in the dashboard as an alert. You can also specify the conditions under which an alert is no longer valid and dismiss it from the dashboard.

#### Before you begin

Role required: sn_bcm.program_manager

#### Procedure

1. Navigate to **Threat and Alert Data Feeds** > **Administration** > **Alert Rules**.
2. Select **New**.
3. On the form, fill in the fields.
   For more information on the Alert Rules form, see Alert Rules form.
4. Select **Submit**.

#### Result

The alert rule is displayed in the **Alert Rules** record page.

### Alert Rules form

Use the Alert Rules form in BCM UIB Workspace to add details about the alert rules.

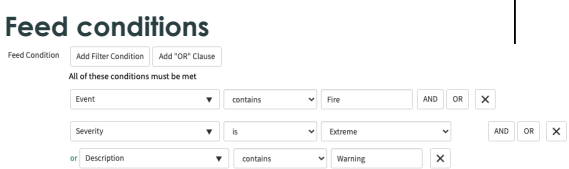
For the description of the field values, see the following table.

**Alert Rules form**

| Field | Description |
|---|---|
| Name | Name of the alert rule. |
| Order | Display order of the alert rule. By default it is 100. |
| Application | Read-only field. The field helps distinguish items relevant to the Crisis map. |
| Category | Category of the record. The value is **BCM**. It helps to identify the BCM-related resources when multiple applications use the component. |
| Active | Option to set the rule active. |
| Description | Details about the alert. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Alert Rules form (continued)

| Field | Description |
|---|---|
| Create Condition | |
| If Resource Impacted | Option for enabling an alert rule if a resource is impacted. |
| Advanced | Option for enabling advanced filter rules with a condition script for the alert rule. |
| Optimize Impact Area | Option to indicate if the map area is to be optimized. Select the check box for optimal performance. |
| Stop On First Match | Option to stop the condition on the first match. |
| Feed Condition | Conditions to filter alerts based on the set rule. Use these filter conditions to set your rules for a feed alert. Setting filter conditions help you to filter those alerts that are critical to your business locations from the thousands of feeds that come from the feed resources you have subscribed. Business locations can be corporate offices, employee locations, datacenters, suppliers, and others.<br>  |
| Advanced Condition Script | Configuration for Advanced Condition Script. This field appears if the **Advanced** option is selected. Enter a script to filter feeds based on a criteria, for example, active alerts. Use the advanced rules option to set a filter rule with a condition script. For example, you can set a condition based on the proximity of the crisis to your asset locations. You can also make the rule active. |
| Dismiss Condition | |
| When Feed Deleted | Option to indicate that the alert must be dismissed from the dashboard, if the feed is deleted. |
| Advanced | Option for enabling advanced filter rules with a condition script for the alert rule. |
| When Resources Not Impacted | Option to indicate that the alert must be dismissed from the dashboard, if there are no resources impacted. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Alert Rules form (continued)**

| Field | Description |
|---|---|
| Feed Condition | Conditions to filter alerts based on the set rule. |
| Advanced Condition Script | Configuration for Advanced Condition Script. This field appears if the **Advanced** option is selected. Enter a script to filter feeds based on a criteria, for example, active alerts. |

### Configure an alert action in Crisis map

Configure an alert action in UIB Workspace for the Crisis map application.

#### Before you begin

Role required: sn_bcm.program_manager

#### Procedure

1. Navigate to **Threat and Alert Data Feeds** > **Administration** > **Alert Actions**.
   You have the following two alert actions that are available within the base system.

| Name | Description |
|---|---|
| Notify | Used to send email notifications to stakeholders and the asset managers that are within the impact radius. |
| Declare Crisis | Used to declare a combination of alert and critical assets as a crisis event. |

2. To add a new alert action, select **New**.
3. On the form, fill in the fields.
   For more information on the fields, see Alert Action form.
4. Select **Submit**.
   You can follow up on the alert actions from the Crisis map dashboard.

#### Result

The alert action is displayed in the **Alert Actions** record page.

### Alert Action form

Use the Alert Action form in BCM UIB Workspace to add details about the alert actions.

For the description of the field values, see the following table.

**Alert Action form**

| Field | Description |
|---|---|
| Title | Title of the alert action. |
| Description | Detailed description of the alert action. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Alert Action form (continued)**

| Field | Description |
|---|---|
| Name | Name of the action in the Crisis map dashboard. |
| Action name | Unique name for the alert action. |
| Run once | Option to indicate the execution of the action one or more times from the dashboard. |
| Type | Type of action to be executed. Available options are:<br>• **Task**<br>• **Script**<br>• **Flow** |
| Task type | Task type for the alert action. For example, Asset task, Catalog task. |
| Application | Read-only field. The field is used as a flag to filter the items relevant to crisis management from a common list of actions. |
| Active | Option to indicate that the alert action is active. |
| Order | Display order that you can follow on the dashboard. |
| Run automatically | Option for enabling the action to be executed automatically based on a condition. |
| Roles | User roles who can execute the task successfully. |
| Display Fields | Fields to be displayed in the response actions after the actions are executed. |
| Condition | Conditions to execute the actions. |
| Task script | Task script to be executed when the user selects an action control on the dashboard. |

## Setup by system administrators

If you are the system administrator, you can set up the Business Continuity Management application by performing certain setup tasks.

Setting up the common administrative tasks requires configuring the pre-requisite data. The following configurations are required to set up the business continuity workspace for different users who would be using the workspace:

- To update the number of the records for a reference field, see Update the number of the records for a reference field.
- To update the number of the element definitions for dependency assessment, see Update the number of the element definitions for dependency assessment.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- To set up an approval configuration in the Business Continuity Management (BCM) application, see Approval configuration.
- To refer to the BCM application menu options, see Application menu options for Business Continuity Management users.

### Update the number of the records for a reference field

Update the number of the records that are displayed for a reference field in the Business Continuity Management (BCM) Workspace. You can configure the *referenceFieldLoadLimit* system property to control the number of the records that are displayed for each reference field on the grid configuration pages.

## Before you begin

Role required: admin

## About this task

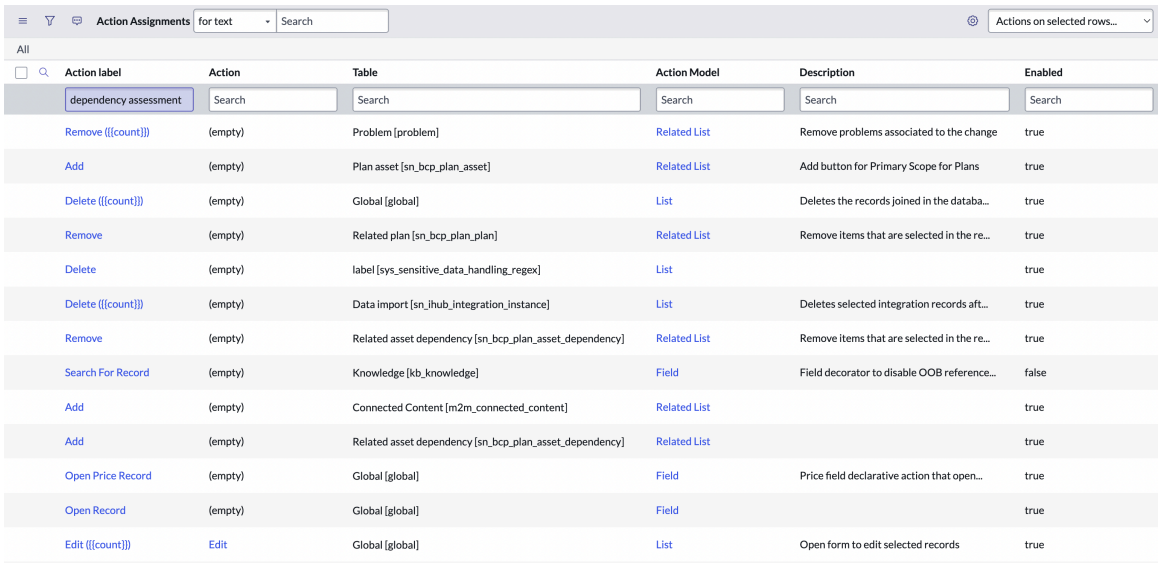
You can configure the *referenceFieldLoadLimit* system property for the reference fields on the following tabs:

- **RTO Impact Assessment** tab, **RPO Impact Assessment** tab, and **Dependency Assessment** tab in a Business Impact Analysis
- **Recovery Tasks** tab in a Plan
- **Impacts** tab and **Event Tasks** tab in an Exercise

## Procedure

1. Navigate to **All** > **sys_declarative_action_assignment.list** in the BCM application instance.

   A list view of the Action Assignments table is displayed as shown in the following example.



Action Assignments | for text | Search | Actions on selected rows...

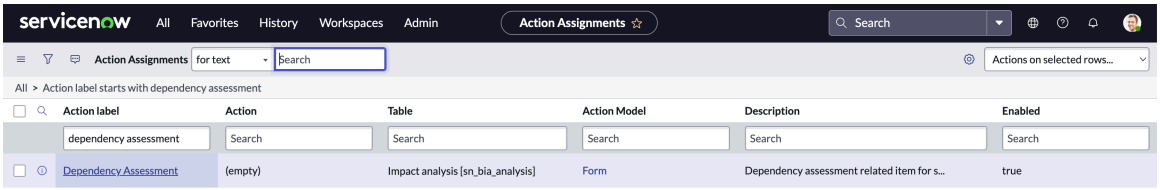
All

| Action label | Action | Table | Action Model | Description | Enabled |
|---|---|---|---|---|---|
| dependency assessment | Search | Search | Search | Search | Search |
| Remove ({{count}}) | (empty) | Problem [problem] | Related List | Remove problems associated to the change | true |
| Add | (empty) | Plan asset [sn_bcp_plan_asset] | Related List | Add button for Primary Scope for Plans | true |
| Delete ({{count}}) | (empty) | Global [global] | List | Deletes the records joined in the databa... | true |
| Remove | (empty) | Related plan [sn_bcp_plan_plan] | Related List | Remove items that are selected in the re... | true |
| Delete | (empty) | label [sys_sensitive_data_handling_regex] | List | | true |
| Delete ({{count}}) | (empty) | Data import [sn_ihub_integration_instance] | List | Deletes selected integration records aft... | true |
| Remove | (empty) | Related asset dependency [sn_bcp_plan_asset_dependency] | Related List | Remove items that are selected in the re... | true |
| Search For Record | (empty) | Knowledge [kb_knowledge] | Field | Field decorator to disable OOB reference... | false |
| Add | (empty) | Connected Content [m2m_connected_content] | Related List | | true |
| Add | (empty) | Related asset dependency [sn_bcp_plan_asset_dependency] | Related List | | true |
| Open Price Record | (empty) | Global [global] | Field | Price field declarative action that open... | true |
| Open Record | (empty) | Global [global] | Field | | true |
| Edit ({{count}}) | Edit | Global [global] | List | Open form to edit selected records | true |

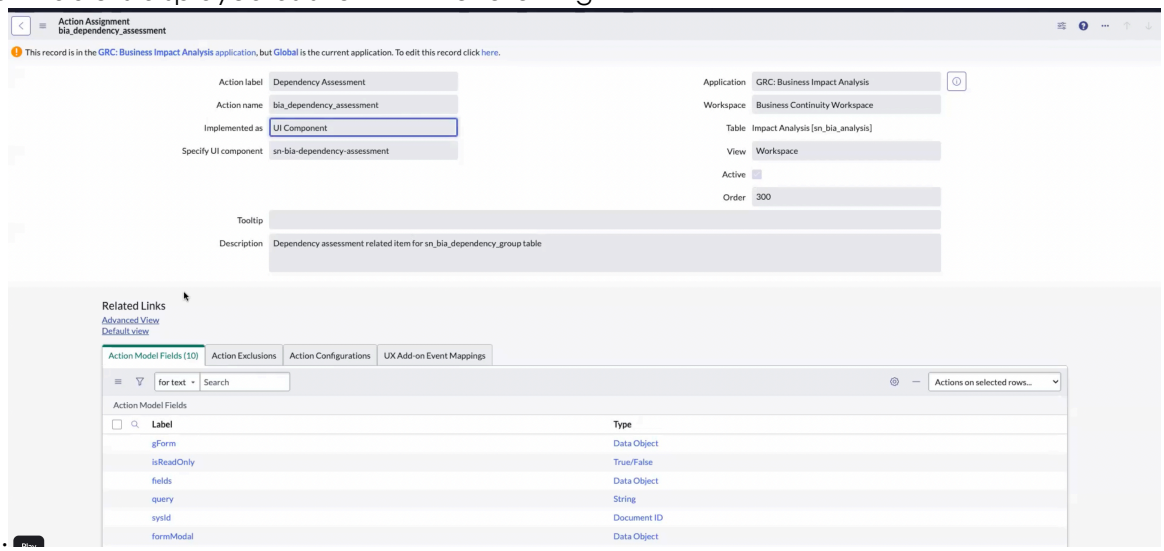
2. In the **Action label** column, enter the name of the assessment action and select the assessment.

   A sample search string for the assessment is displayed in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

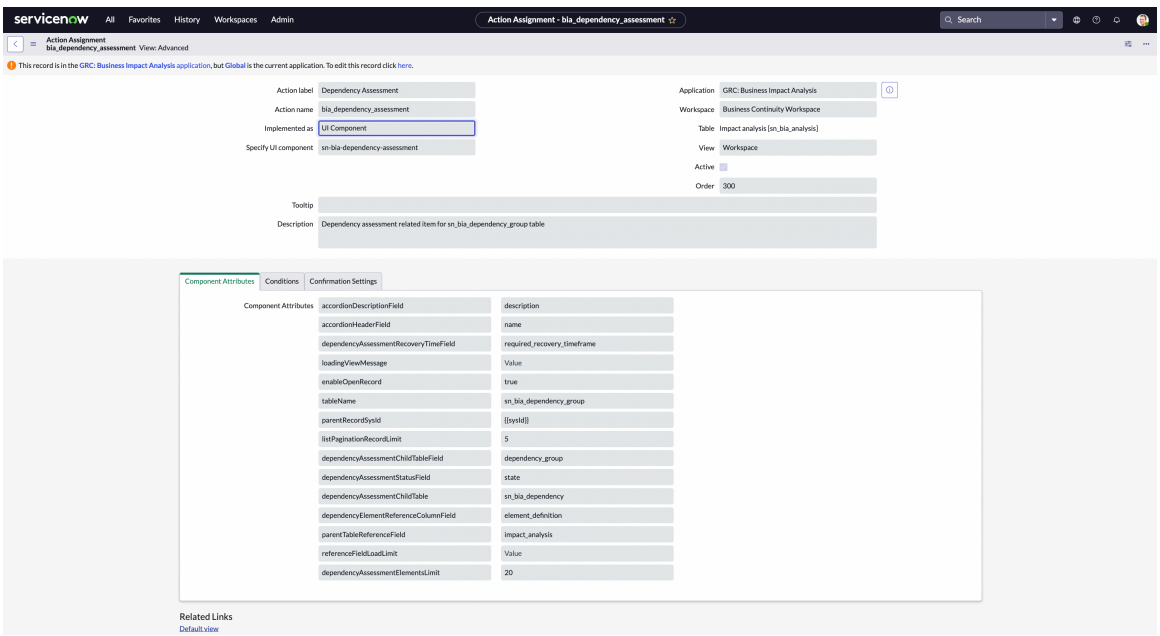



When you select the assessment, the form view of the Action Assignment table is displayed as shown in the following example.




3. In the form view of the Action Assignment table, select **Advanced View**.

   After you've selected the **Advanced View**, the properties for the selected action are displayed in the **Component Attributes** tab as shown in the following example.



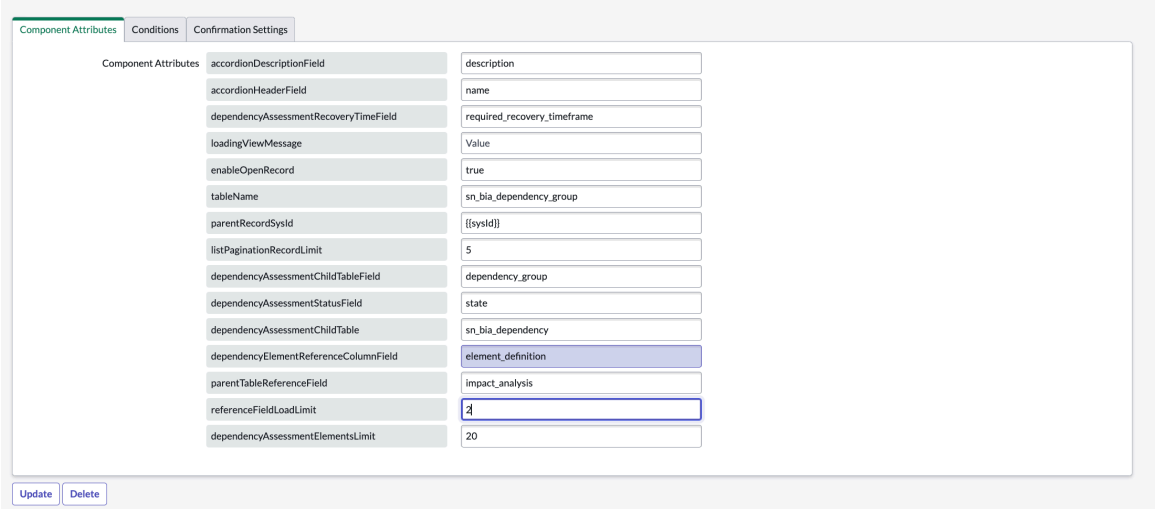

   The following informational message is displayed on the screen: `To edit this record, click Here.`

4. To update the *`referenceFieldLoadLimit`* property for the selected record, select **Here** in the informational message.

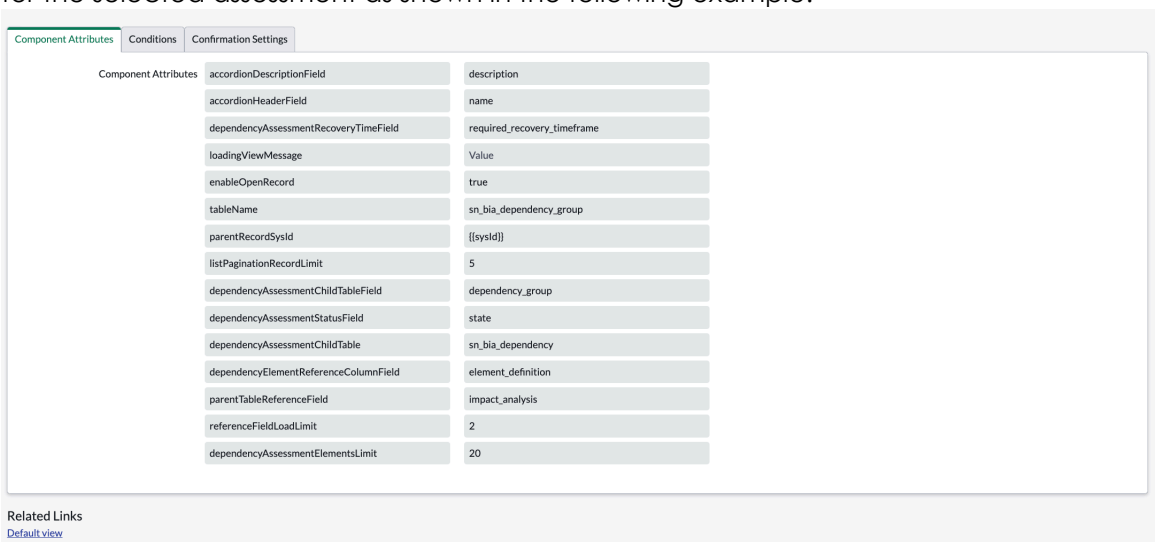
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

By updating the *referenceFieldLoadLimit* property, you can control the number of the records on the grid configuration page.

A sample configuration of the *referenceFieldLoadLimit* property is displayed in the following example.



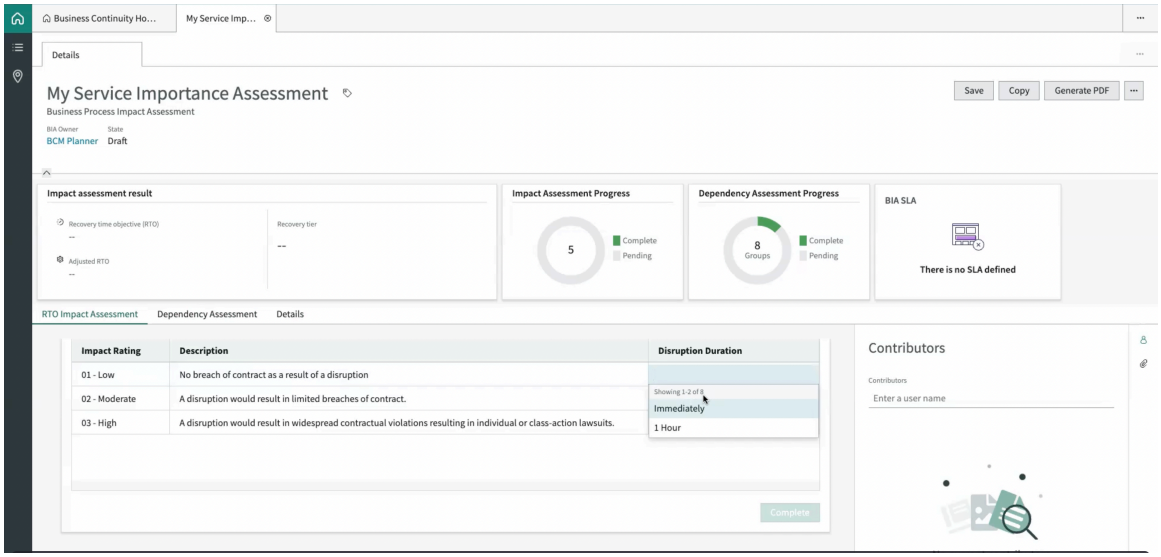

5. Select **Update**.
   You've configured the *referenceFieldLoadLimit* property for the selected assessment as shown in the following example.




**Note:** As outlined in the context of this task, you can set the *referenceFieldLoadLimit* property to control the number the reference fields on different grid configuration pages.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following example shows the updated number of the records for the **Disruption Duration** field in the **RTO Impact Assessment** tab.




## Update the number of the element definitions for dependency assessment

Update the number of the element definitions that are displayed on the **Dependency Assessment** tab in the Business Continuity Management (BCM) Workspace. You can configure the *dependencyAssessmentElementsLimit* system property to control the number of the element definitions that are used for the dependency assessment in a business impact analysis.

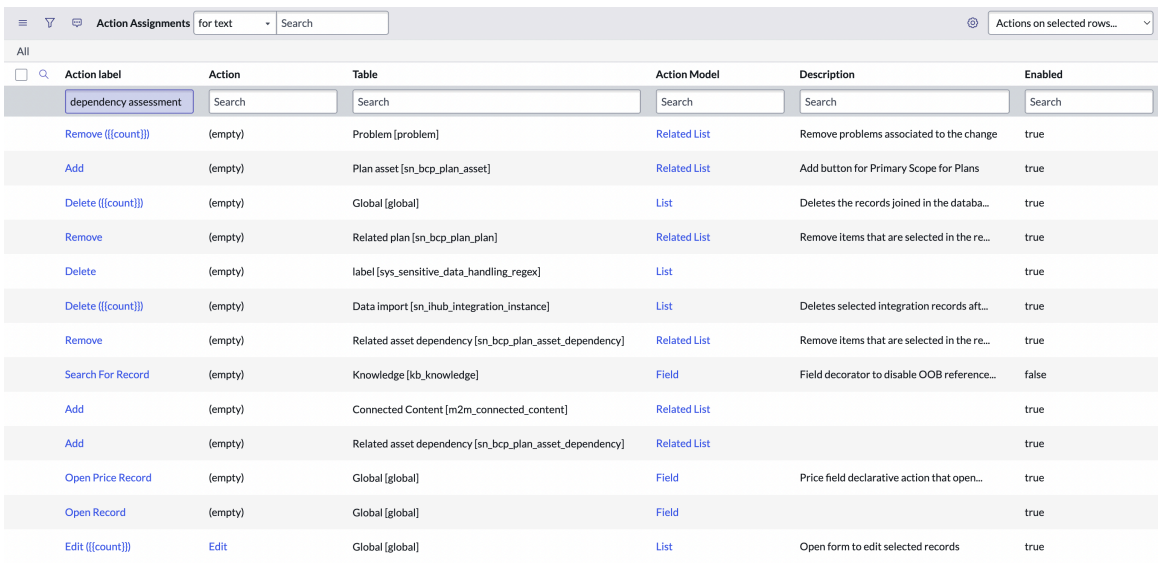
### Before you begin

Role required: admin

### Procedure

1. Navigate to **All** > **sys_declarative_action_assignment.list** in the BCM application instance.

   A list view of the Action Assignments table is displayed as shown in the following example.

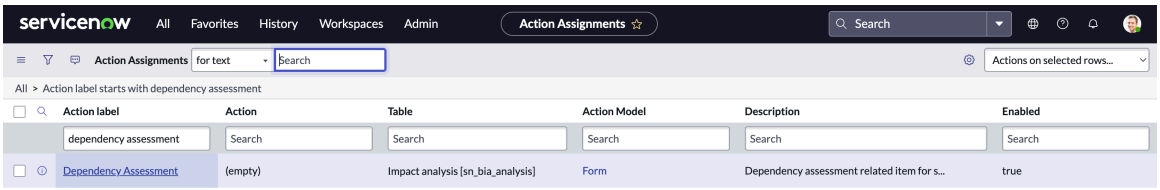



| Action label | Action | Table | Action Model | Description | Enabled |
|---|---|---|---|---|---|
| dependency assessment | Search | Search | Search | Search | Search |
| Remove {{{count}}} | (empty) | Problem [problem] | Related List | Remove problems associated to the change | true |
| Add | (empty) | Plan asset [sn_bcp_plan_asset] | Related List | Add button for Primary Scope for Plans | true |
| Delete {{{count}}} | (empty) | Global [global] | List | Deletes the records joined in the databa... | true |
| Remove | (empty) | Related plan [sn_bcp_plan_plan] | Related List | Remove items that are selected in the re... | true |
| Delete | (empty) | label [sys_sensitive_data_handling_regex] | List | | true |
| Delete {{{count}}} | (empty) | Data import [sn_ihub_integration_instance] | List | Deletes selected integration records aft... | true |
| Remove | (empty) | Related asset dependency [sn_bcp_plan_asset_dependency] | Related List | Remove items that are selected in the re... | true |
| Search For Record | (empty) | Knowledge [kb_knowledge] | Field | Field decorator to disable OOB reference... | false |
| Add | (empty) | Connected Content [m2m_connected_content] | Related List | | true |
| Add | (empty) | Related asset dependency [sn_bcp_plan_asset_dependency] | Related List | | true |
| Open Price Record | (empty) | Global [global] | Field | Price field declarative action that open... | true |
| Open Record | (empty) | Global [global] | Field | | true |
| Edit {{{count}}} | Edit | Global [global] | List | Open form to edit selected records | true |

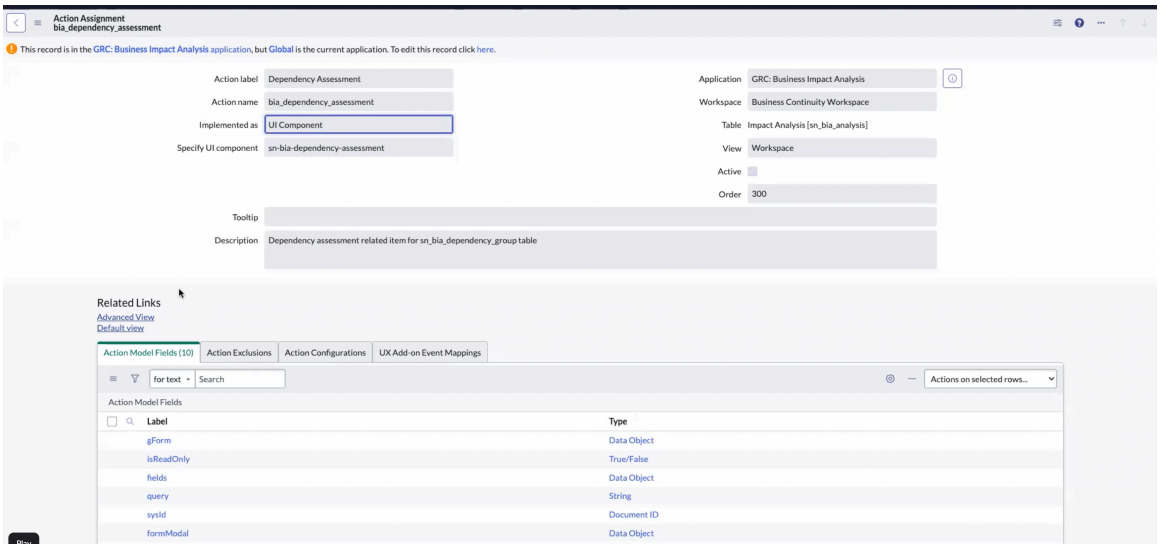
2. In the **Action label** column, enter the name of the assessment such as **Dependency Assessment** and select the assessment.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A sample text string is displayed in the following example.

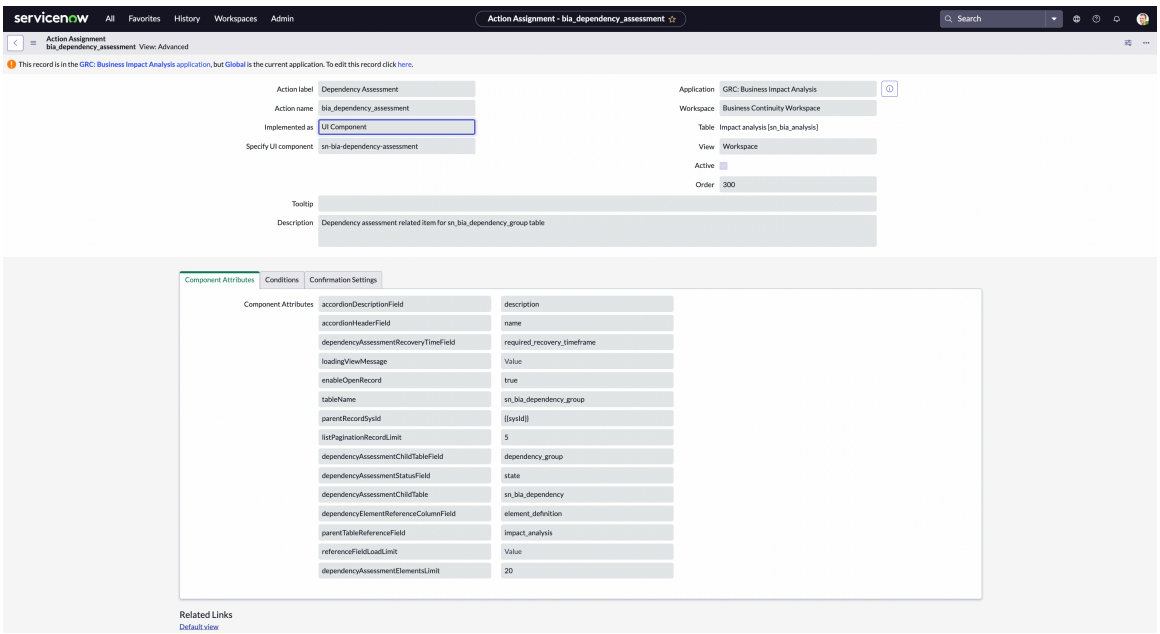



When you select the assessment, the form view of the Action Assignment table is displayed as shown in the following example.




3. In the form view of the Action Assignment table, select **Advanced View**.

After you've selected the **Advanced View**, the properties for the selected action are displayed in the **Component Attributes** tab as shown in the following example.



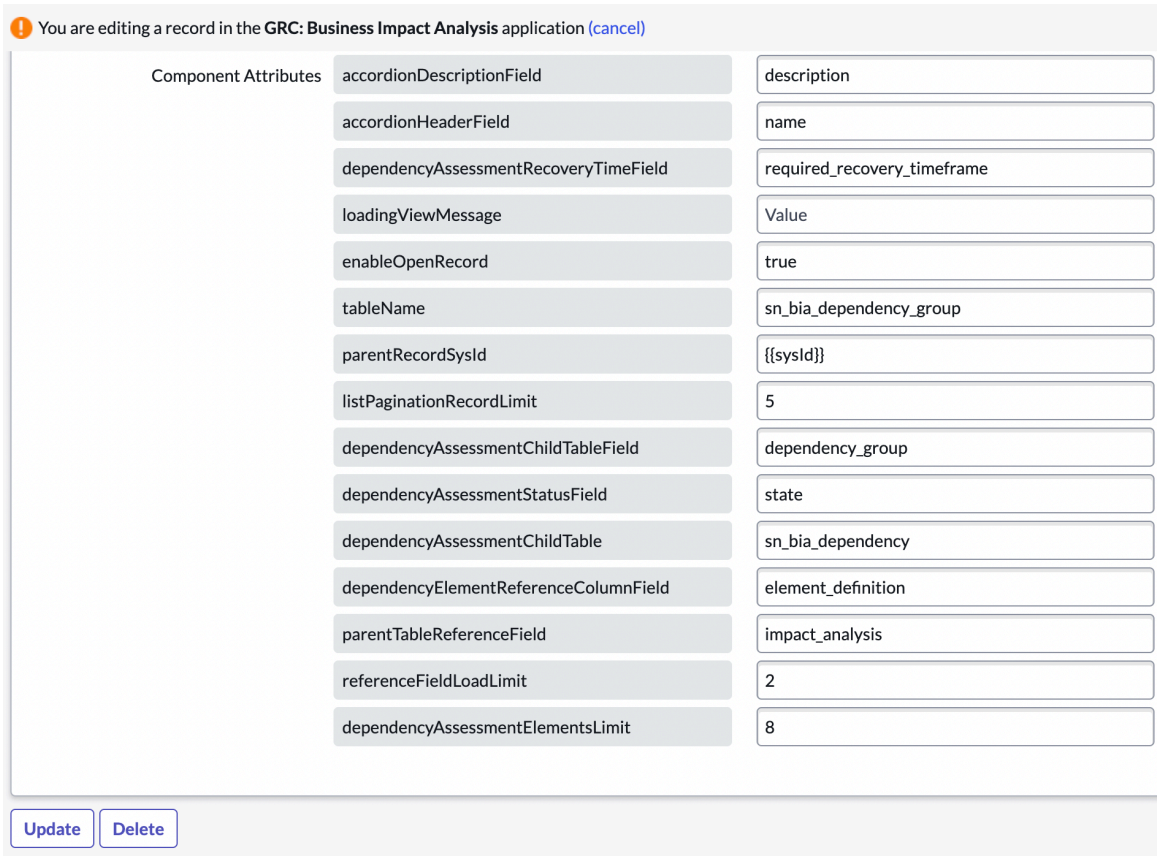

The following informational message is displayed on the screen: `To edit this record, click Here.`

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To update the *dependencyAssessmentElementsLimit* property, select **Here** in the informational message.

   By updating the *dependencyAssessmentElementsLimit* property, you can control the number of the element definitions for the dependency assessment.

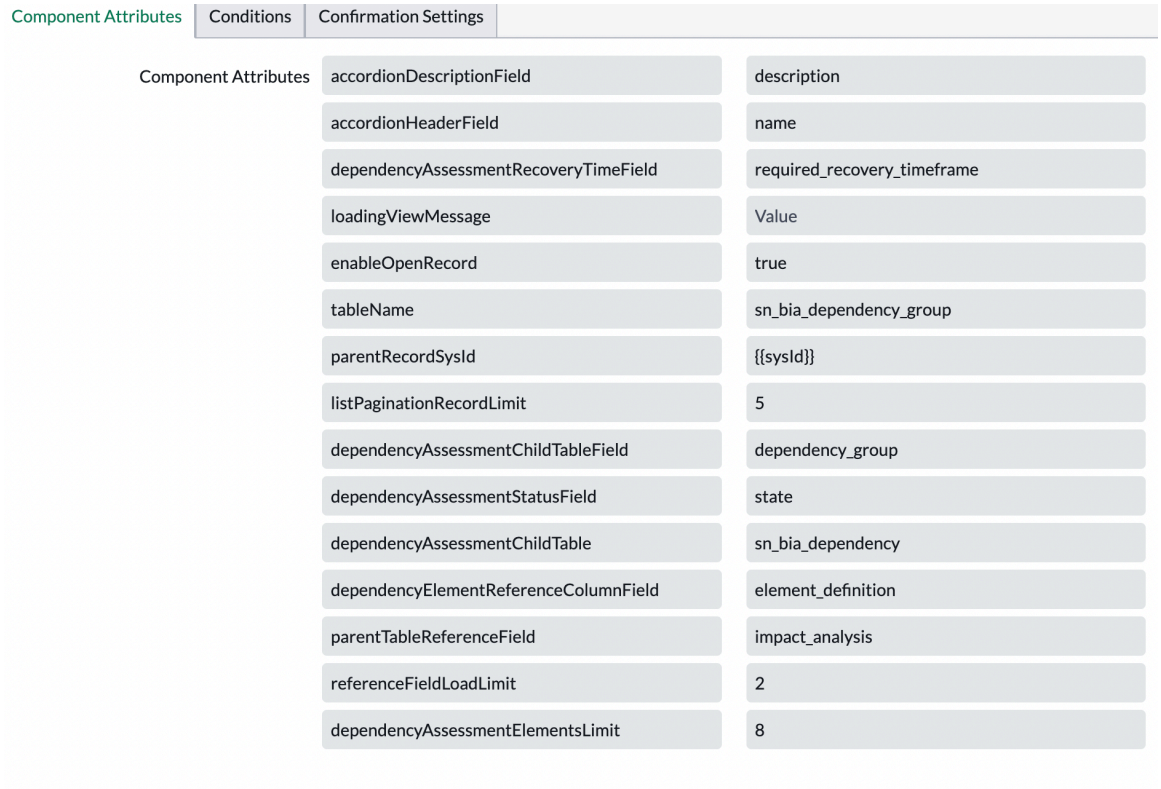
   A sample configuration of the *dependencyAssessmentElementsLimit* property is displayed in the following example.




5. Select **Update**.

   You've configured the *dependencyAssessmentElementsLimit* property as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The updated number of the element definitions are displayed on the **Dependency Assessment** tab.

### Application menu options for Business Continuity Management users

The table lists the application menu options that are available for the main users of the business continuity management application to view and navigate.

## BCM application menu options

For detailed information on user roles, see Roles installed table.

| | | |
|---|---|---|
| | BCM Admin | As a BCM administrator, you can access all menu options from the Business Continuity menu:<br>• Business Continuity Workspace<br>• Business Impact Analysis<br>• Planning<br>• Crisis Management<br>• BIA Configuration<br>• Plan Configuration<br>• General Administration |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| | | |
|---|---|---|
|  | BCM program manager | As a BCM program manager you can view and access the following menu options:<br>• Business Continuity Workspace<br>• To create an impact analysis: **Business Continuity** > **Business Impact Analysis** > **Impact Analysis**<br>• To create a plan: **Business Continuity** > **Planning** > **Plans**<br>• To create an event: **Business Continuity** > **Crisis Management** > **Events** |
|  | BCM planner | As a BCM planner you can view and access the following menu options:<br>• Business Continuity Workspace<br>• To create an impact analysis: **Business Continuity** > **Business Impact Analysis** > **Impact Analysis**<br>• To create a plan: **Business Continuity** > **Planning** > **Plans**<br>• To create an event: **Business Continuity** > **Crisis Management** > **Events** |
|  | BCM viewer | To view the workspace: **Business Continuity** > **Business Continuity Workspace** |

## Setup for the UI Builder

You can set up and extend the BCM Workspace pages and components by using the UI Builder.

## About UI Builder

UI Builder is a drag-and-drop Web user interface builder that uses the Next Experience Components and custom web Components.

To build and customize your Workspace pages and components, you must have the ui_builder_admin role.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Navigating to UI Builder in your instance

In your application instance, you can navigate to **All > Now Experience Framework > UI Builder** and select an experience that you want to work in from the UI Builder home page.

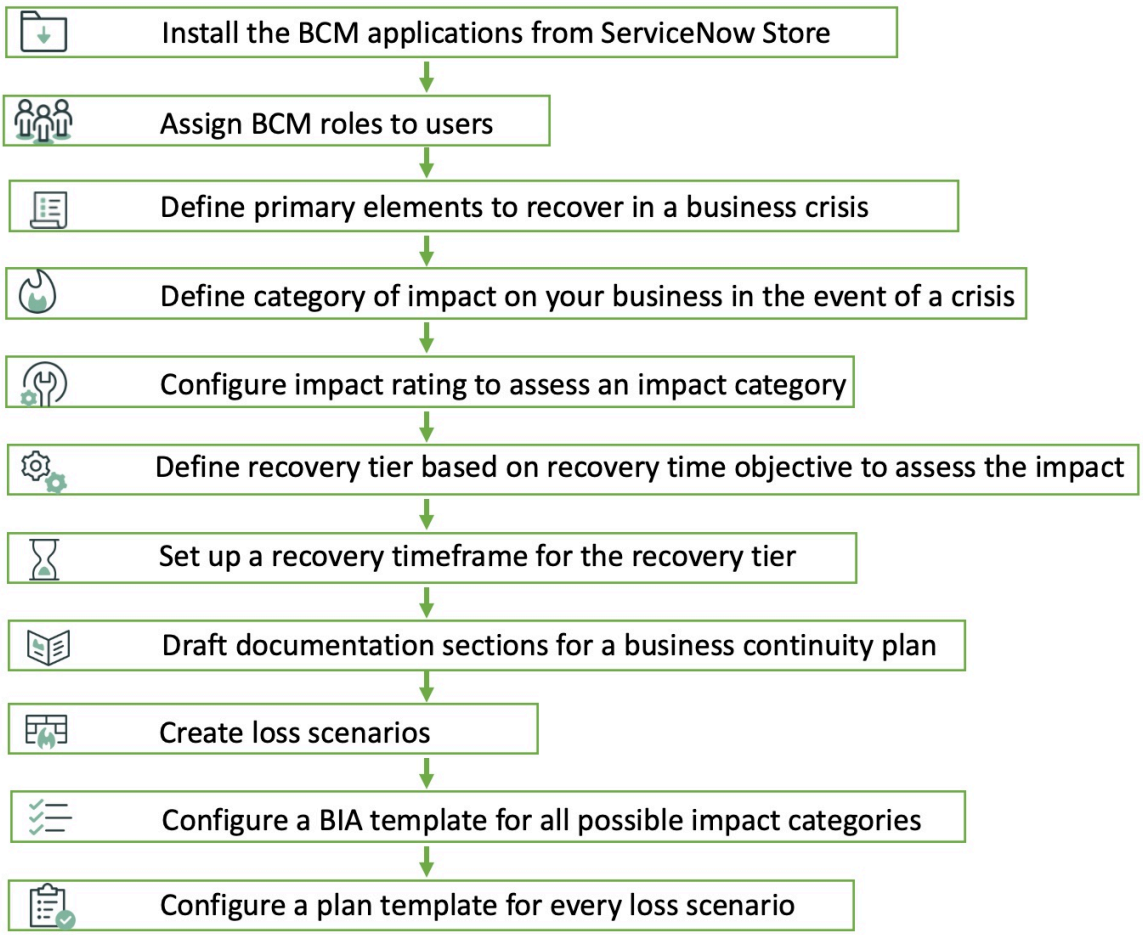
For more information on how to use a UI Builder, see UI Builder quick start.

## Business Continuity Management implementation

Use the steps in the Business Continuity Management application checklist to download the Business Continuity Management from the ServiceNow Store, and get it ready for operation.

The flow of implementation steps in the checklist are illustrated here.

**Graphical flowchart of BCM implementation checklist**




## Information on the checklist

For information on the steps that are mentioned in the *Graphical flowchart of BCM implementation checklist*, see the following sections:

- To install Business Continuity Management from ServiceNow Store, see Install Business Continuity Management from ServiceNow Store.
- To learn about BCM roles, see Components installed with Operational Resilience.
- To learn about the administration setup listed in the flowchart, see General administration setup for BCM. Refer to this section for information on the following tasks:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

  - To define the primary elements to recover in a business crisis, see Configure an element definition for the business impact analysis.
  - To define the category of impact on your business in the event of a crisis, see Configure an impact category for the business impact analysis.
  - To configure an impact rating to assess an impact category, see Configure an impact rating to assess the impact category.
  - To define a recovery tier based on the recovery time objective to assess the impact, see Configure a recovery tier for the business impact analysis.
  - To set up a recovery timeframe for the recovery tier, see Set up a recovery timeframe for a recovery tier.
  - To draft the documentation sections for a business continuity plan, see Configure the documentation section for a business continuity plan.
  - To create a loss scenario, see Configure a loss scenario in your business continuity plan.
- To configure a BIA template for the impact categories, see Configure a business impact analysis (BIA) template.

  **Note:** When you create a business impact analysis in BCM UIB Workspace, you can assign a BCM lead to the analysis in the BIA form itself.

- To configure a plan template for a loss scenario, see Configuring the plan template for the business continuity plan.

  **Note:** When you create a business continuity plan in BCM UIB Workspace, you can assign a BCM lead to the plan in the BCP form itself.

## Managing business continuity workflow tasks in BCM UIB Workspace

You can use the features and capabilities of the Business Continuity Management application to perform activities such as business impact analysis, business continuity planning, exercise management, crisis management, and so on.

### Performing business continuity tasks in BCM UIB Workspace

Perform the tasks that are outlined in this section to manage business continuity for your organization. You can create a business impact analysis, business continuity plan, an exercise event, or manage a crisis event in Business Continuity Workspace (also known as BCM UIB Workspace).

See the following sections for performing business continuity tasks in BCM UIB Workspace:

- For tasks related to a business impact analysis, see Structured workflows for Business Impact Analysis in BCM UIB Workspace.
- For tasks related to a business continuity plan, see Structured workflows for Business Continuity Planning in BCM UIB Workspace.
- For tasks related to an exercise event, see Structured workflows for Exercise Management in BCM UIB Workspace.
- For tasks related to a crisis event, see Structured workflows for Crisis Management in BCM UIB Workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Structured workflows for Business Impact Analysis in BCM UIB Workspace

Perform the tasks that are outlined in this section to create a business impact analysis in Business Continuity Workspace (also known as BCM UIB Workspace).

Typically, the business impact analysis owner performs the following tasks:

- Create a business impact analysis. For more information, see Create a business impact analysis.
- Assess the impact categories and submit the analysis for a review and approval.

  **Note:** If an approval record is already created for a BIA, the **Approve** or **Reject** buttons are not displayed in the BIA form.

  For more information, see Assess the impact categories and dependencies.
- As the BCM lead, approve the BIA. For more information, see Approve the business impact analysis.
- Generate and save the PDF of the analysis for reference.

## Additional information on Business Impact Analysis

- For information on the **Business impact analysis** tab in the Home page, see Home page view.
- For information on business impact analysis, see Business impact analysis.
- For information on the administrative tasks in business impact analysis, see Setup for a business impact analysis.

### Impact categories and ratings

Impact categories are the types of an impact that you can assess during a business impact analysis. The BCM administrator of an organization is responsible for defining the impact categories and the timeframe during which an organization may experience a downtime. This information is used to determine the recovery time objective and recovery point objective of the assets.

## Broad classification of the impact categories

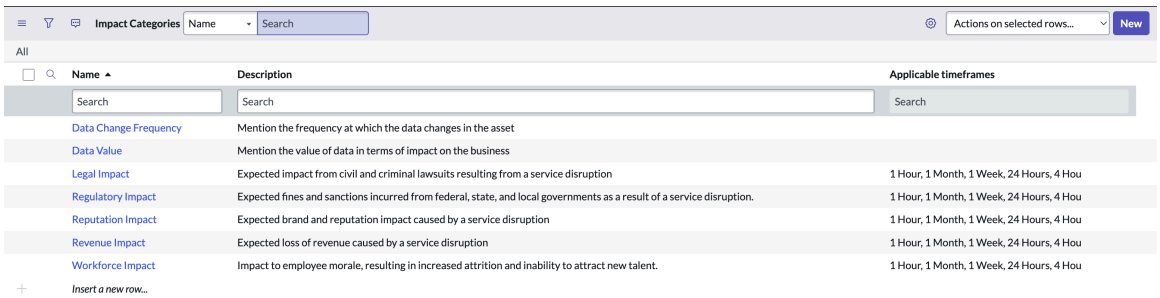
When a business service, process, or application experiences downtime due to a disruptive event, its impact can be classified in various broad categories:

- Legal impact: Classified as an impact with legal implications such as a civil lawsuit or fines that result from a service disruption.
- Regulatory impact: Classified as an impact due to a change in the existing regulation or the introduction of a new policy.
- Reputation impact: Classified as an impact to the brand image and reputation of a company.
- Revenue impact: Classified as an impact due to financial losses or low revenues.
- Workforce impact: Classified as an impact of a disruptive event on the workforce. For example, a company experiences an increased attrition rate and low employee morale post the pandemic.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

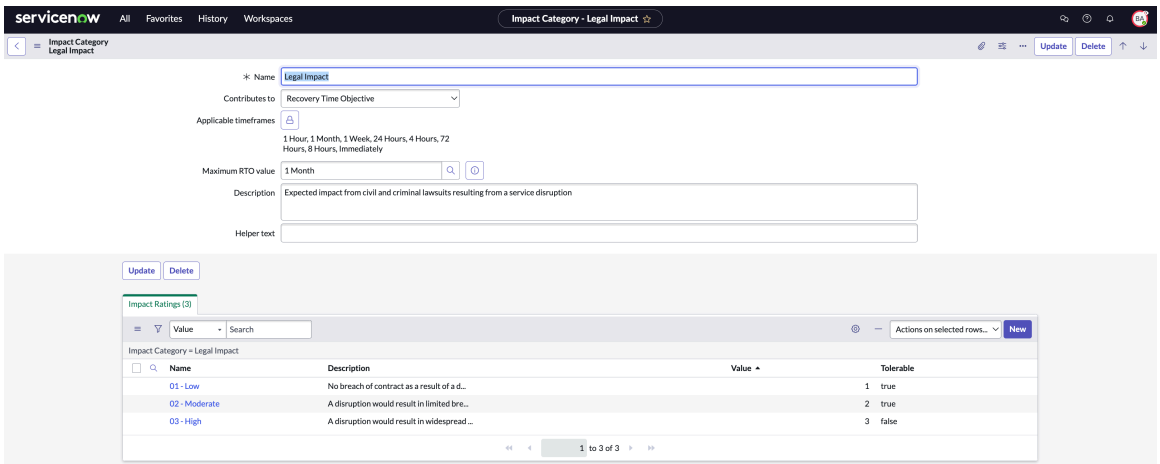
## Impact categories in BCM

With the BCM administrator role, you can view the impact categories that are installed with demo data and set up new impact categories in the **Impact categories** module of the BCM application. The following example shows the impact categories that are installed with demo data in an instance.




## Configuration of an impact category

The BCM administrators can configure or modify the impact categories by adding key information about the impact. The following example shows the configuration details of an impact category in an instance.




The BCM administrators can configure the following details of a new impact category:

Name

Classify the impact of a downtime for your service, process, or applications by adding an appropriate name for the impact such as Legal or Reputational impact.

Contributes to

Select whether the impact contributes to recovery time objective or recovery point objective.

Applicable timeframes

Set the applicable timeframe for the impact category.

Maximum RTO value

Define the maximum RTO value for the impact category.

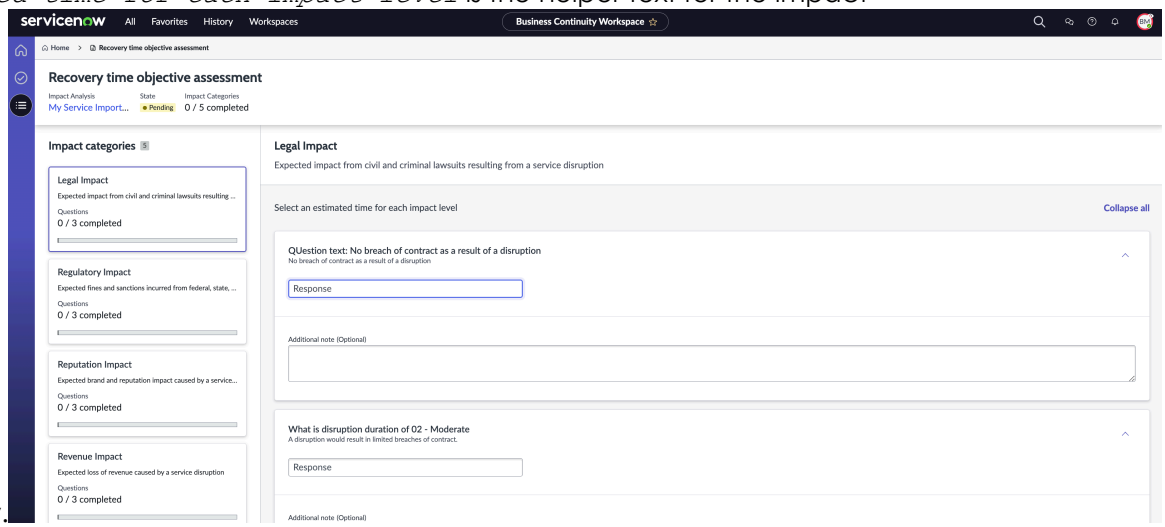
Description

Add description for the impact category.

Helper text

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Add the helper text that provides a hint to the users on how to respond to the assessment questions. The helper text is then displayed for the user in the business impact analysis record. In the following example, *Select an estimated time for each impact level* is the helper text for the impact category.

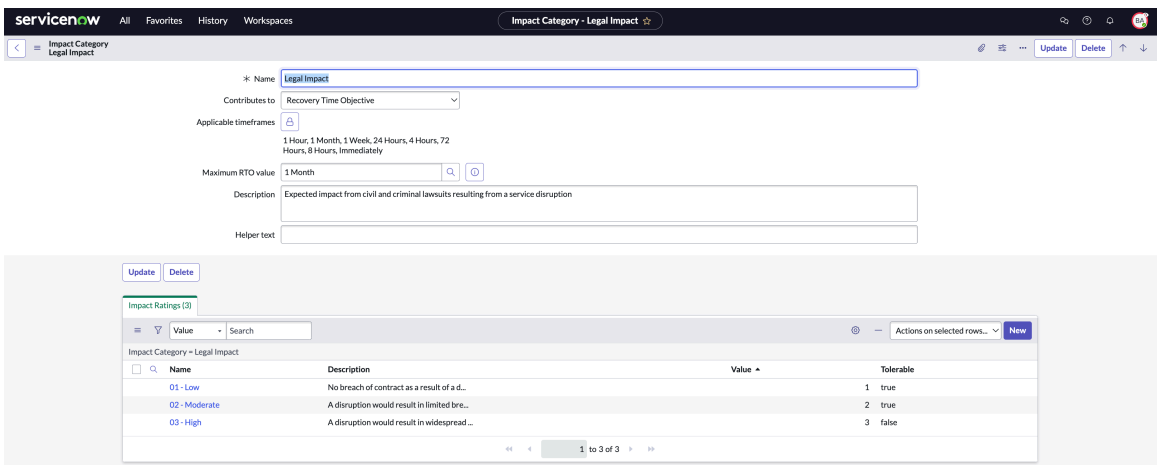



## Impact category configuration by the administrators

For more information on how to configure an impact category with the sn_bcm.admin role, see Configure an impact category for the business impact analysis.

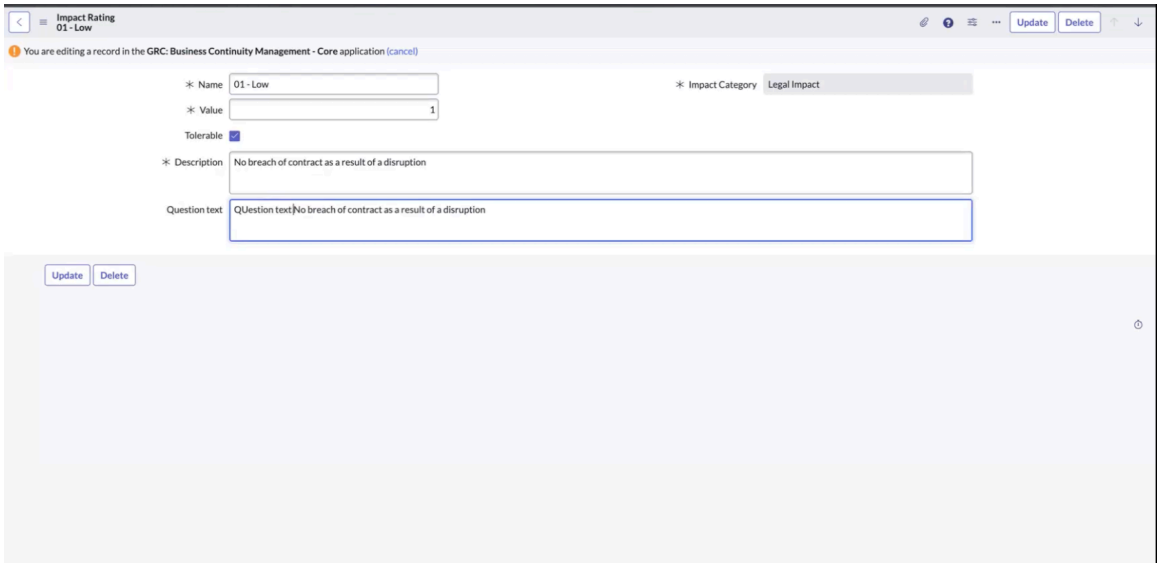
## Impact ratings in BCM

If you have the BCM administrator role, you can view the impact ratings that are installed with demo data and define specific impact ratings in the **Impact ratings** module. The following example shows the impact ratings that are installed with demo data for an impact category.




The impact ratings for an impact category are shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## Configuration of an impact rating

The BCM administrators can configure the following details of an impact rating for the business impact analysis:

Name

Assign a unique name to the impact rating.

Impact Category

Classify the impact category that the impact rating is associated with.

Value

Assign a unique numerical value to each impact rating. The same value can not be reused for any other impact rating in the BCM application.

Tolerable

Select the option for enabling the RTO impact as tolerable. This check box appears only if the impact category contributes to the recovery time objective.

Description

Add the description about the impact rating.

Question text

Revise the question text in the Impact Rating record for the recovery time objective of an impact category. The revised question is then displayed in the RTO assessment form of the business impact analysis record.

## Impact rating configuration by the administrators

For more information on how to configure an impact rating with the sn_bcm.admin role, see Configure an impact rating to assess the impact category.

### Recovery time objective, Recovery point objective, and Recovery tiers

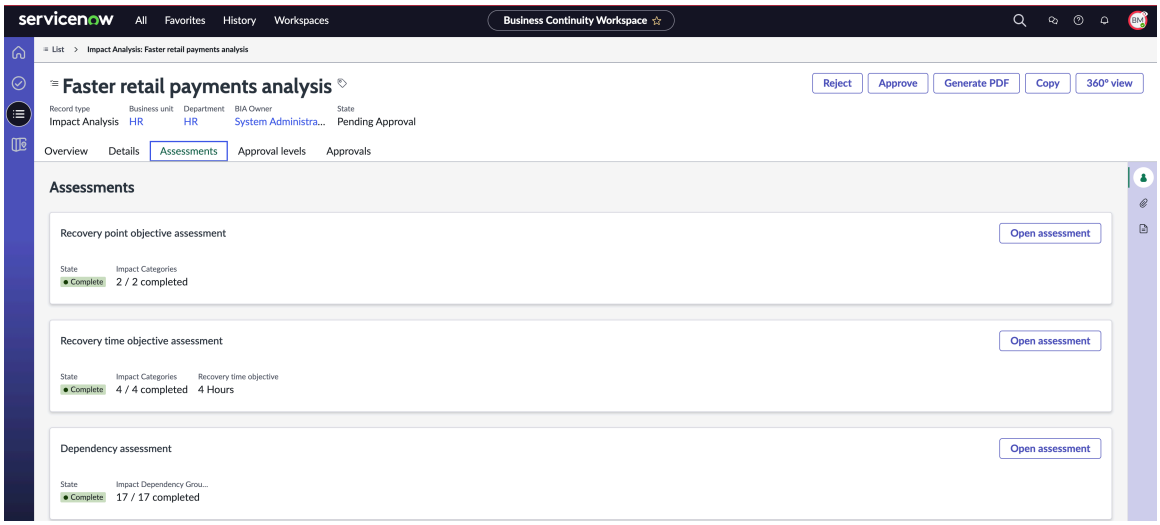
Due to unforeseen disruptive events, the business processes in your organization can face a downtime. It is important to classify your business processes in the recovery tiers and calculate the amount of time and amount of data loss that your organization can handle without significant effect on the operations.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

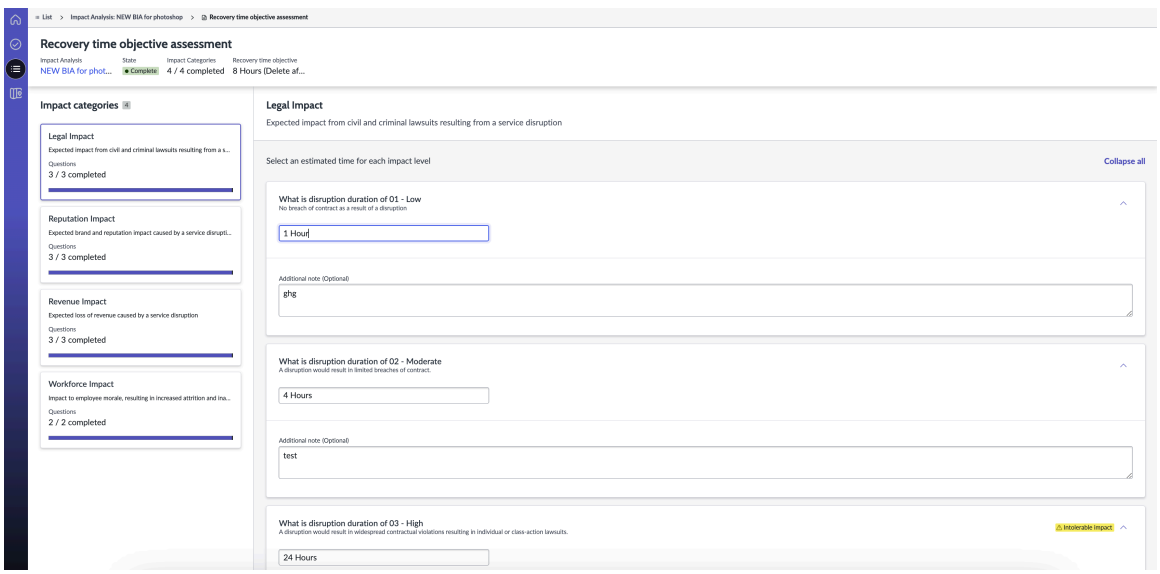
## Recovery time objective

Recovery time objective (RTO) is the maximum amount of time a computer, system, network, or application takes to recover after an outage event or data loss without causing much effect to your business operations.

The business users and IT owners can perform business impact analysis and technical impact analysis respectively by responding to the assessment in the BIA component in the BCM UIB Workspace. A sample view of the **Assessments** tab is shown in the following example.




If you are the business user, you can estimate the recovery time objective for your business services and processes by responding to the Recovery time objective assessment in the **Assessments** tab. The questions are displayed in the **Recovery time objective assessment** tab according to the configuration set up by the BCM administrator. A sample Recovery time objective assessment with demo data is shown in the following example.



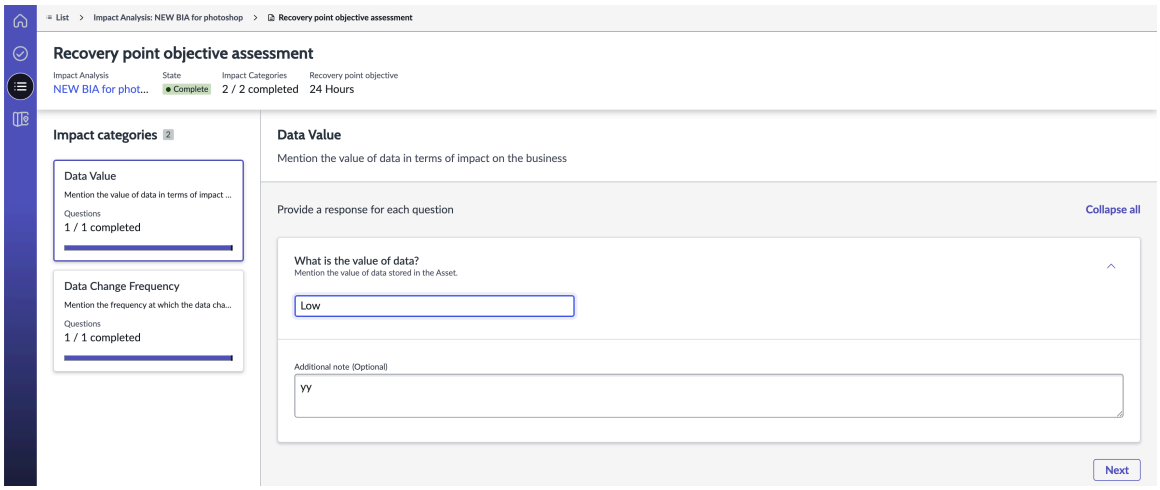

## Recovery point objective

Recovery point objective (RPO) defines the maximum acceptable data loss that a business process can handle without significant effect on operations.

If you are the IT owner, you can estimate the recovery point objective for your data applications and systems by responding to the Recovery point objective assessment in the

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

BIA. Based on the configuration set up by the BCM administrator, the questions are displayed in the **Recovery time objective assessment** tab as shown in the following example.



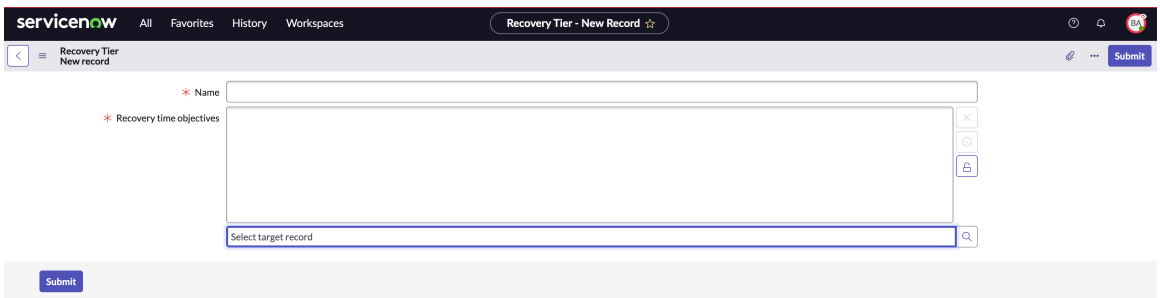

## Recovery tier

If you are the BCM administrator, you can classify a set of business applications that follow a similar range of recovery time objective (RTO) values in one type of recovery tier. For example, for the Mission Critical recovery tiers, recovery time objectives can be Immediately, one Hour, and four Hours.

The recovery tiers and their associated recovery time objectives are displayed in the following example.




The BCM administrator can configure a recovery tier and set its recovery time objective as shown in the following example.




Recovery tiers are also associated with other organizational expectations such as levels of support, escalation, and communication. Recovery tiers are used in the following areas:

- BIA scores and impact assessment result
- Element recovery times

Although there is no limitation to the number of the recovery tiers, an organization can set 4 to 6 recovery tiers. Recovery tiers are automatically calculated on BIAs and element RTO by selecting the nearest recovery tier maximum time.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Recovery tiers can be classified as per their importance and criticality:

- Mission Critical
- Business Critical
- Essential
- Non-essential
- Critical
- Non-Critical

## Recovery tier configuration by the administrators

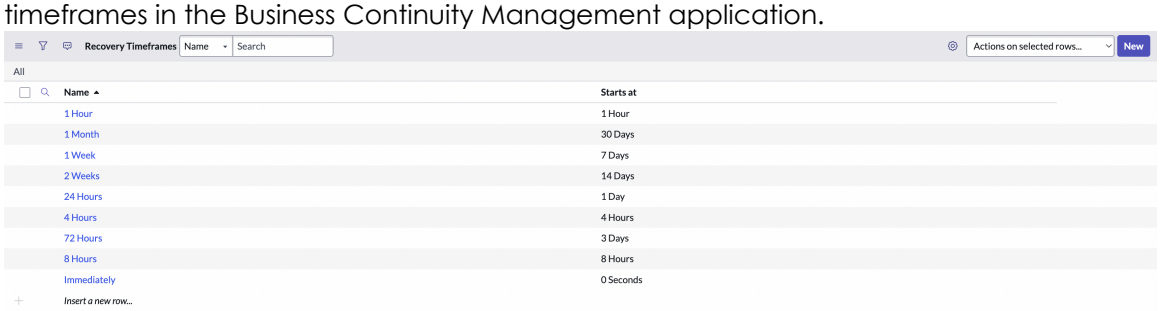
For more information on how to configure a recovery tier in the Business Continuity Management application, see Configure a recovery tier for the business impact analysis.

## Recovery timeframe

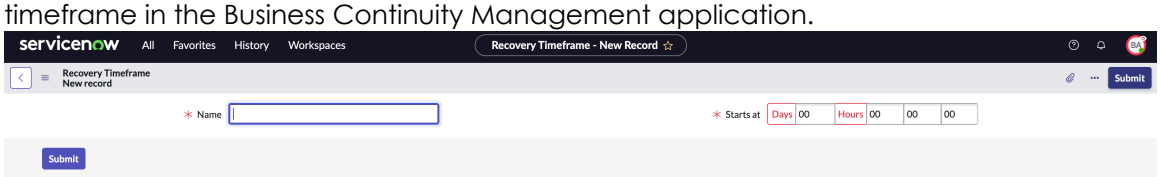
You can set up the recovery timeframe for a recovery tier. It is the timeframe that starts from when a disruptive event happens to the time when your business can resume usual operations. The BCM administrator can configure the recovery timeframe and its start time. You can configure different recovery timeframes as shown in the following example:

- Immediately
- 1 Hour
- 4 Hours
- 8 Hours
- 24 Hours
- 72 Hours
- 1 Week
- 2 weeks

The following example shows the configured recovery timeframes in the Business Continuity Management application.




The following example shows the configuration of a recovery timeframe in the Business Continuity Management application.




For more information on how to configure a recovery timeframe in the Business Continuity Management application, see .

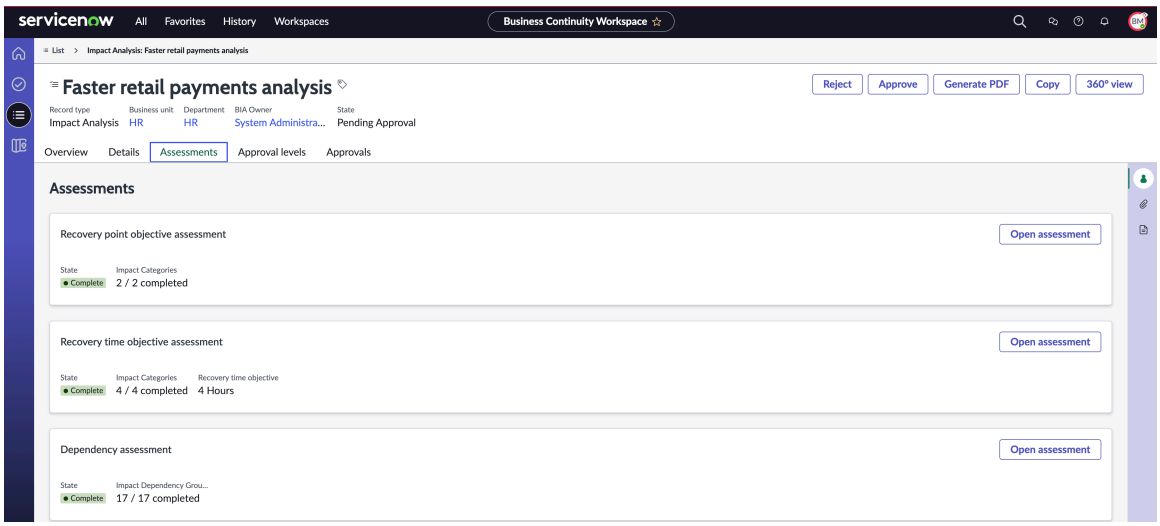
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Calculating the recovery time objective and recovery point objective

The BCM application provides an assessment questionnaire for calculating the recovery time objective (RTO) and recovery point objective (RPO) in the business impact analysis (BIA). As a pre-requisite to the BIA, the BCM administrator defines the impact ratings and sets up the assessment questions. After receiving the responses to the assessment, the BCM application calculates the RTO and RPO.

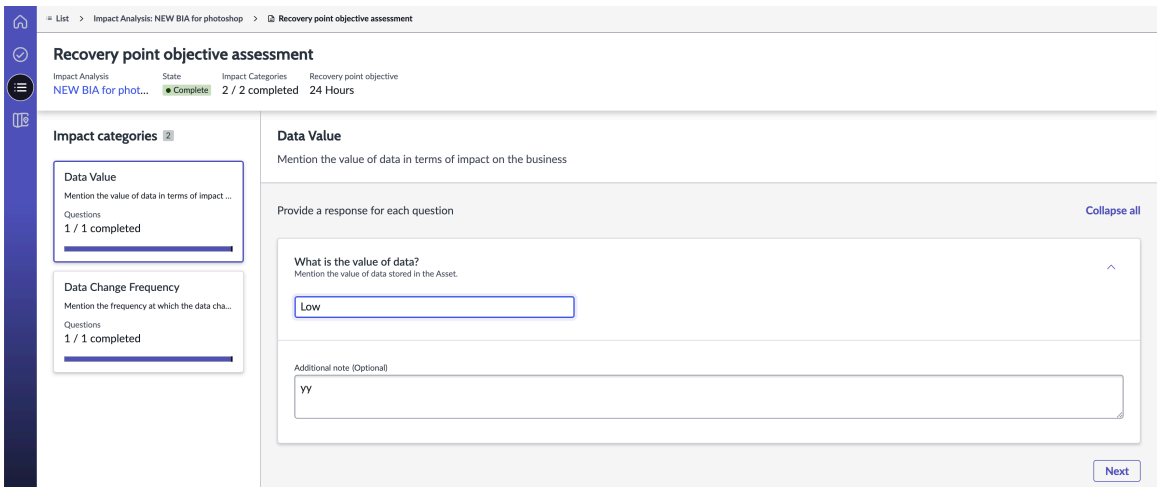
## Assessment tab in the business impact analysis record

The business users and IT owners can perform business impact analysis and technical impact analysis respectively by responding to the assessment in the BIA component in the BCM UIB Workspace. A sample view of the **Assessments** tab is shown in the following example.




## Recovery point objective assessment

If you are the IT owner, you can estimate the recovery point objective for your data applications and systems by responding to the Recovery point objective assessment in the BIA. Based on the configuration set up by the BCM administrator, the questions are displayed in the **Recovery point objective assessment** tab as shown in the following example.

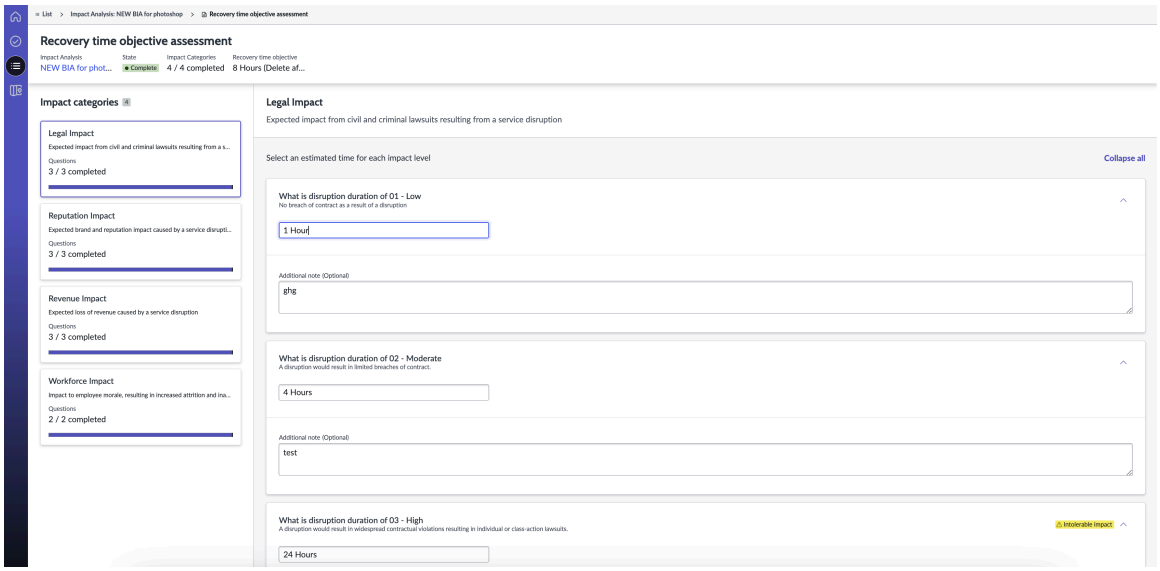



## Recovery time objective assessment

If you are the business user, you can estimate the recovery time objective for your business services and processes by responding to the Recovery time objective assessment in the

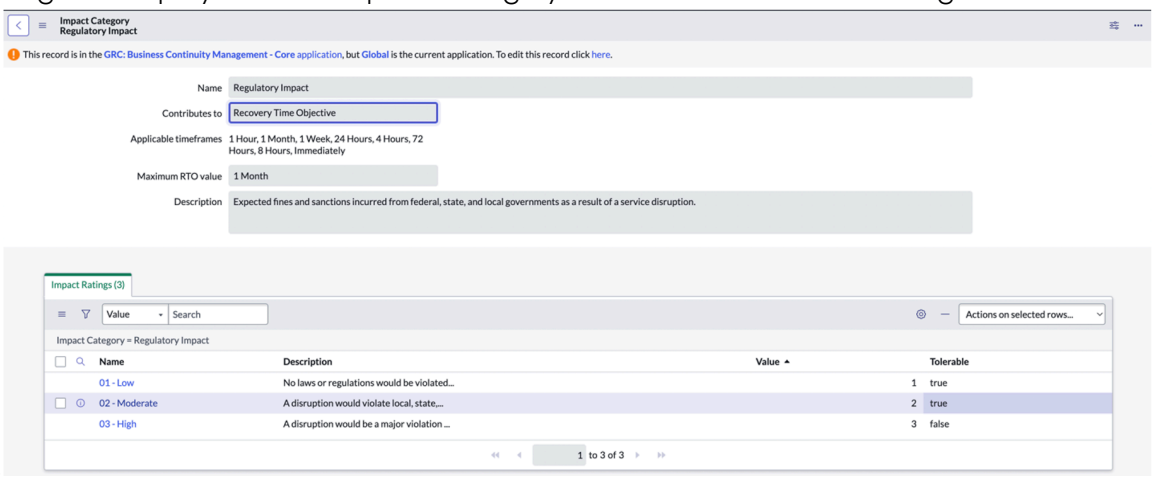
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Assessments** tab. The questions are displayed in the **Recovery time objective assessment** tab according to the configuration set up by the BCM administrator. A sample Recovery time objective assessment with demo data is shown in the following example.




## Administrator view for the impact category and impact ratings

The BCM administrator can configure the assessment questionnaire to include one or multiple impact ratings such as **Low**, **Moderate**, or **High** for an impact category. The impact ratings are displayed in the Impact Category view as shown in the following example.



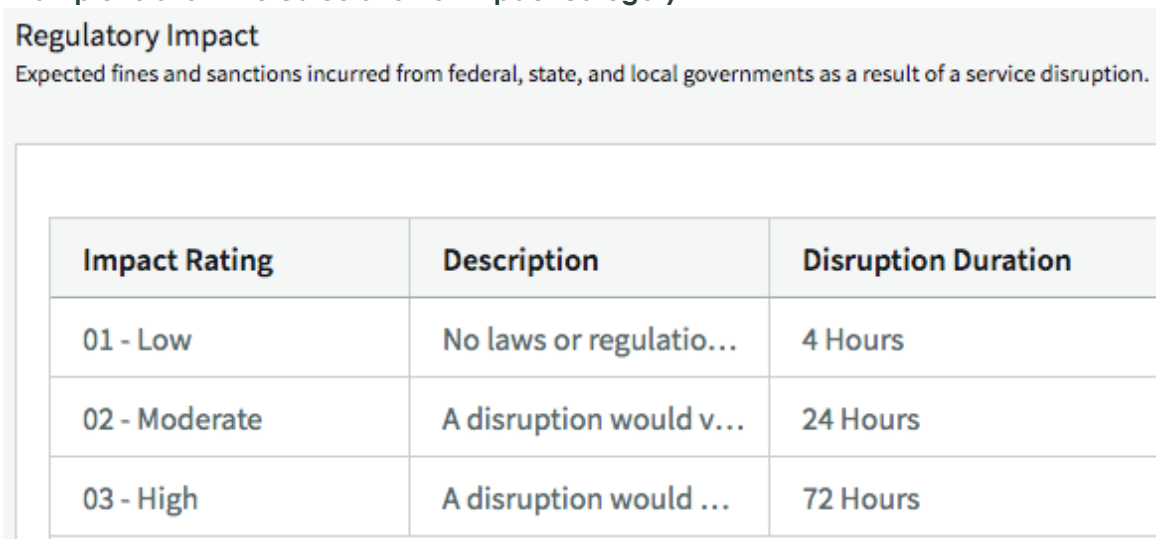

The BCM administrator can specify a threshold of non-tolerance for the impact ratings per impact category. The disruption duration for the first non-tolerable impact category is selected for the recovery time objective (RTO). The impact ratings have the following specified values:

- Low = 1
- Moderate = 2
- High = 3

See the following example for the calculation of the impact category.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Example to show the calculation of impact category**




## Calculating the Recovery time objective (RTO)

As a business user, when you respond to the assessment questionnaire, the BCM application automatically calculates the Recovery time objective (RTO) for your business processes and services.

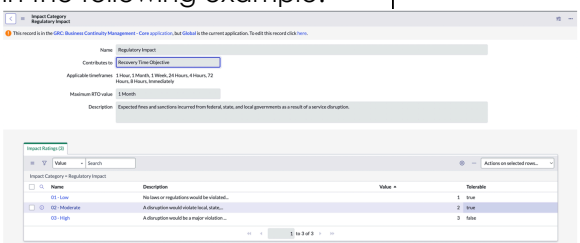
Consider the following scenario for a sample RTO calculation. The BCM administrator has configured an intolerable impact rating for the Revenue impact category and defined the intolerable impact. If you are the business impact analysis owner, you must identify the timeline at which the revenue impact may go beyond $1M. See the sample RTO calculation for different scenarios as shown in the following table.

**Sample RTO calculation**

| Scenario | Non-tolerable impact | Description |
|---|---|---|
| Scenario 1 | In the Impact Ratings table, the **Tolerable** field is set to **false**. | If the administrator has specified that Low regulatory impact is non-tolerable, its corresponding disruption duration is set as the recovery time objective (RTO).<br><br>In this example, the disruption duration for the **01 - Low** impact rating is set to 4 hours. Therefore, the recovery time objective (RTO) for the impact category is above 4 hours.<br><br>Even if the moderate impact disruption duration is shorter, the calculation selects the value from the first alphanumerically sorted |

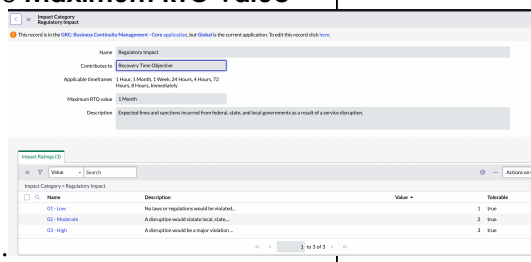
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Sample RTO calculation (continued)

| Scenario | Non-tolerable impact | Description |
|---|---|---|
| | | impact rating that has the **Tolerable** field set to **false**. |
| Scenario 2 | In the Impact Ratings table, the **Tolerable** field is set to **false**. | If the administrator has specified that Moderate regulatory impact is non-tolerable, its corresponding disruption duration is set as the recovery time objective (RTO).<br><br>In this example, the disruption duration for **02 - Moderate** impact is set to 24 hours. Therefore, the recovery time objective (RTO) for the impact category is above 24 hours. |
| Scenario 3 | In the Impact Ratings table, the **Tolerable** field is set to **false**. | If the administrator has specified that High regulatory impact is non-tolerable, its corresponding disruption duration is set as the recovery time objective (RTO) as shown in the following example.<br><br>  <br><br>In the tabular example, the disruption duration for **03 - High** impact is set to 72 hours. Therefore, the recovery time objective for the impact category is above 72 hours. |
| Scenario 4 | The **Tolerable** field for the Low, Moderate, and High impact ratings is set to **true**. | If the administrator has set all the impact ratings as tolerable, the value specified in the **Maximum RTO value** field in the template is selected as the recovery time objective (RTO). |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Sample RTO calculation (continued)**

| Scenario | Non-tolerable impact | Description |
|---|---|---|
| | | In the following example, the administrator has set all the impact ratings as tolerable. Therefore, the recovery time objective (RTO) is one month as per the value specified in the **Maximum RTO value** field.  |

Calculation of overall impact assessment result for a BIA

When you update the **Disruption Duration** of an impact category, the RTO of the BIA is automatically updated. The RTO of the BIA is set as the lowest tolerable downtime from each impact category.

For example, consider a BIA having four impact categories – Legal, Reputation, Workforce, and Regulatory. When you update the disruption duration value of the legal impact category, then the RTO value of the BIA is recalculated based on the lowest tolerable disruption duration from each impact category. The Recovery Tier varies from organization to organization and is set based on the recalculated RTO value.

| RTO value | Recovery Tier |
|---|---|
| Immediate | Mission Critical |
| 1 Hour | Mission Critical |
| 4 Hours | Mission Critical |
| 8 Hours | Business Critical |
| 24 Hours | Business Critical |
| 72 Hours | Essential |
| 1 Week | Essential |
| 2 Weeks | Non-Essential |
| 1 Month | Non-Essential |

Calculation of category score from impact analysis questions for an impact category that contributes to Recovery Point Objective (RPO)

If the impact category contributes to **RPO**, then evaluate each impact analysis question in that RPO category based on the value of your data like business critical, operation critical, business essential, or operation essential. The maximum value among all the questions of that RPO is considered as the Category Score

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

of that Impact Category and stored in the Impact Category Results table [sn_bia_category_result].

### States and UI actions associated with a business impact analysis

When you create a business impact analysis, certain UI actions are associated with each state.

## States and their UI associated actions in a business impact analysis

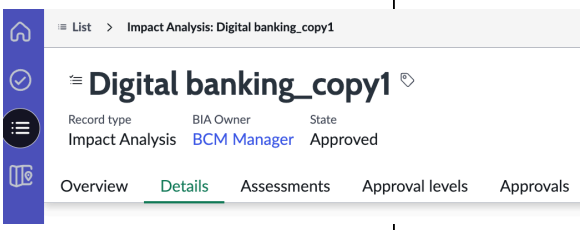
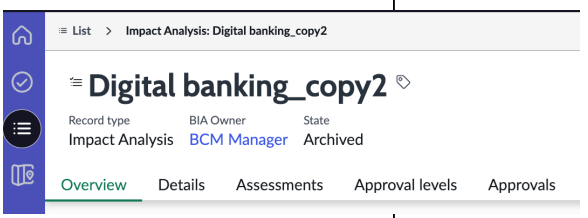
The states and their UI associated actions in a business impact analysis are described in the following table.

**States and their UI associated actions in a business impact analysis**

| State of the business impact analysis | UI action | Description of the action |
|---|---|---|
| **Draft** | In the Business Impact Analysis record Lists view, select **New**.<br><br>**Note:** You can also navigate to the **Business Impact Analysis** section of the Home page and select **Create BIA**. | When you select **New** in the Create New Impact analysis form or **Create BIA** in the Home page, a record is created in the **Draft** state by default.<br><br>On the **Details** tab, you can add details of the business impact analysis (BIA). On the **Assessments** tab, you can respond to the Recovery point objective assessment, Recovery time objective assessment, and Dependency assessment. |
| **In review** | Select **Submit for review**. | When you select **Submit for review** in the Create New Impact analysis form, the state of the business impact analysis is updated to **In review**. |
| **Pending approval** | Select **Submit for approval**. | When you select **Submit for approval** in the Create New Impact analysis form, the state of the business impact analysis is updated to **Pending approval**. |
| **Approved** | Select **Approve**. | When you select **Approve** in the Create New Impact analysis form, the state of the business impact analysis is updated to **Approved**. The **Overview** tab displays |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and their UI associated actions in a business impact analysis (continued)**

| State of the business impact analysis | UI action | Description of the action |
|---|---|---|
| | | the progression of the states as shown in the following example.<br>  <br>When the business impact analysis is in the **Approved** state, it is in the read-only format. You can only view the Recovery point objective assessment, Recovery time objective assessment, and Dependency assessment in the **Approved** state. |
| **Archived** | In the Create New Impact analysis form, select **Archive**. | When you select **Archive** in the Create New Impact analysis form, the state of the business impact analysis is updated to **Archived** as shown in the following example.<br>  <br>When the business impact analysis is in the **Archived** state, it is available in the read-only format. You can no longer edit the information in these tabs.<br>You can perform the following additional UI actions in the Create New Impact analysis form:<br>Generate PDF<br>Download the PDF of the |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and their UI associated actions in a business impact analysis (continued)**

| State of the business impact analysis | UI action | Description of the action |
|---|---|---|
| | | business impact analysis for reference. The PDF attachment is available in the **Activity** panel on the **Details** tab.<br><br>For more information, see Generate the PDF of a business impact analysis.<br><br>Copy<br><br>Save a copy of the PDF of the business impact analysis for future reference as a template.<br><br>360° view<br><br>Visualize 360° representation of the business impact analysis such as its name, template used, dependencies, and BIA result.<br><br>For more information, see Visualize the 360° relationships for a business impact analysis.<br><br>Delete<br><br>Delete the business impact analysis if you don't need to refer to it anymore.<br><br>Edit<br><br>Edit the business impact analysis in the application. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and their UI associated actions in a business impact analysis (continued)**

| State of the business impact analysis | UI action | Description of the action |
|---|---|---|
| | | Save<br>Save the business impact analysis in the application. |
| **Returned** | Select **Reject**. | If you select **Reject** in the Create New Impact analysis form, the state of the business impact analysis is set to **Returned**. You can edit the business impact analysis in the **Returned** state. You can update and submit it for review again. |

**Note:** A scheduled job runs weekly to move the expired business impact analyses to the **Archived** state.

## Create a business impact analysis

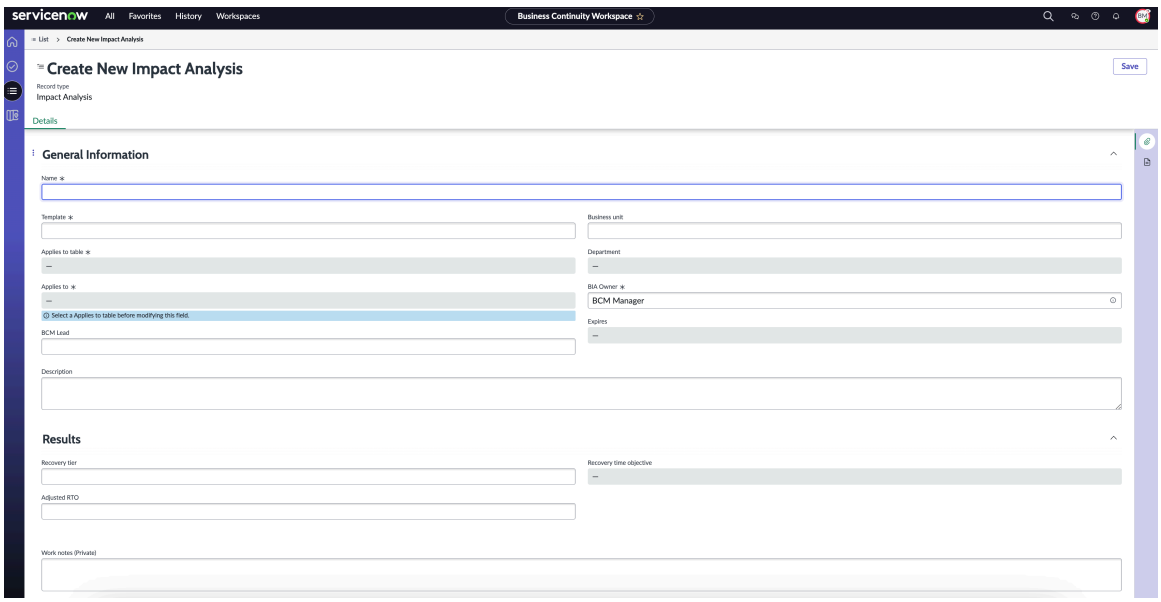
Create a business impact analysis in BCM UI Builder Workspace to get the necessary information for a plan.

### Before you begin

Role required: sn_bia.bia_admin, sn_bcm.program_manager, sn_bcm.planner

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Business Impact Analysis** and select **New**.
   The **Create New Impact analysis** form is displayed as shown in the following example.



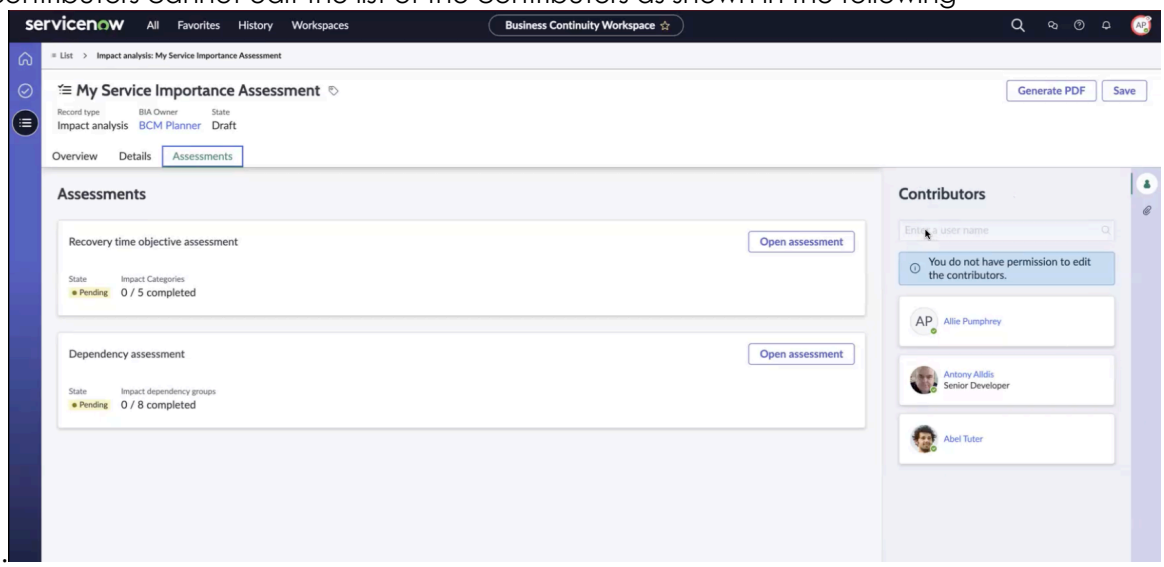

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. On the **Details** tab of the **Create New Impact analysis** form, fill in the required fields. For more information on the fields, see Create New Impact analysis form.
   The business impact analysis is created in the **Draft** state and it is displayed in the List view.
   The state and details of the business impact analysis are displayed in the following tabs:
   - **Overview**: You can view the current state and overall state progression for the business impact analysis.
   - **Details**: You can add the details of the business impact analysis such as its name, template, business unit, department, and so on.
   - **Assessment**: You can fill in responses to the assessment questionnaires for the business impact analysis in the **Recovery time objective assessment**, **Recovery point objective assessment**, and **Dependency assessment** tabs.
4. Launch the **Contributors** panel by selecting the **Contributors** icon in the side-bar and add a contributor from the list to the business impact analysis record.

   If you are the BIA owner or BCM manager, you can add a contributor to the business impact analysis.

   **Note:** Even though the BIA contributors with the sn_bia.bia_contributor role have read access to the BIA, they can complete the assessments on the **Assessment** tab.

   The BIA contributors cannot edit the list of the contributors as shown in the following example.




5. Select **Save**.

   The business impact analysis is saved the **Draft** state and it is displayed in the Business Impact Analysis List view of the records.

### Create New Impact analysis form

Use the Create New Scenario analysis form to add details about the business impact analysis, assessments, approvals, and so on, in BCM UIB Workspace.

## Create New Impact analysis form

For a description of the field values, see the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create New Impact analysis form

| Field | Description |
|---|---|
| Overview tab (Displayed when an analysis is created.) | |
| State | Stepper component for the states of the business impact analysis. |
| Details tab | |
| Name | Name of the business impact analysis. Describe the business impact analysis within 255 characters length. |
| Template | Template that you can use as a model to create the business impact analysis.<br><br>The BIA template has the primary elements (applications, business processes, and locations), impact categories, and the dependent assets identified for the type of assessment. |
| Applies to table | Business process, business application, or any other asset that is assessed in the business impact analysis. This field is auto-filled according to the template selected. |
| Business unit | Table that stores the template's primary element data. |
| Department | Department that uses the business process. You can select the department based on the business unit selected. |
| Applies to | Process that the analysis applies to. |
| BIA Owner | Person who owns and is responsible for completing the business impact analysis. BCM lead can review the business impact analysis. |
| BCM Lead | BCM lead assigned to the analysis. |
| Expires | Expiration date for the analysis. This field is auto-filled. |
| Description | Description of the process. |
| Results | |
| Recovery tier | Recovery tier for the business impact analysis. |
| Adjusted RTO | RTO that is adjusted manually. |
| Recovery time objective | Recovery time objective for the impact analysis. |
| Work notes | Work notes for the business impact analysis. This field is auto-filled. |
| Icons displayed in the side-bar of the record | |
| Contributors | Icon to populate the side-panel in the record. You can add contributors to the business impact analysis from the panel. |
| Attachment | Panel where the PDF of the business impact analysis is attached. |
| Template | Panel to populate the template for the business impact analysis. You can view all or customized templates in this panel. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

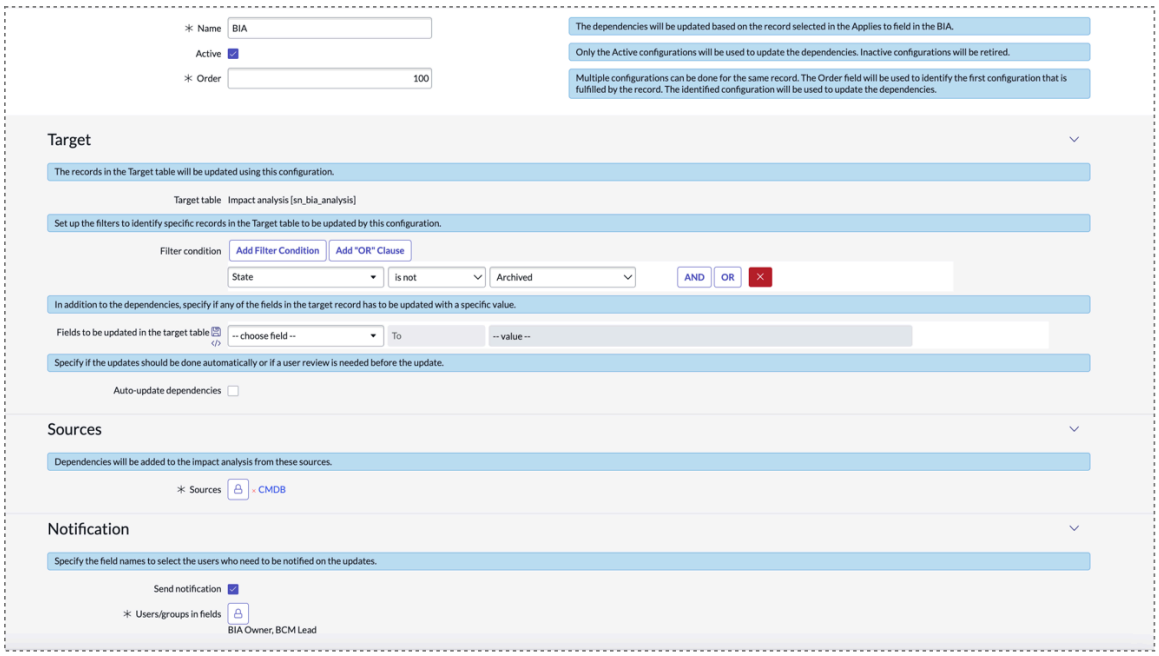
### Schedule an auto-update of the dependencies in the business impact analysis

You can schedule an auto-update of the dependencies in the business impact analysis based on the source data and relationships in the CMDB. You can receive an email notification with details of the BIA dependency updates from the BCM application.

## Scheduling an auto-update of the dependencies

The BCM administrators can schedule an auto-update of the BIA dependencies in the Impact analysis dependency update configuration module, based on the source data and relationships in the CMDB.

The Impact analysis dependency update configuration module is shown in the following example.




When the BCM administrators select the **Auto-update dependencies** option, the BCM application schedules an auto-update of the dependencies in the BIAs. Similarly, when the **Send notification** option is selected, the BCM application sends automated emails to the BIA owners about the dependency updates.

The source for the BIA dependencies is CMDB.

**Note:** The dependencies are fetched for the BIA that is listed in the **Applies to** field of the BIA record such as HR Application BIA, Accounts Receivable BIA.

Setting up the Impact analysis dependency update configuration module is a one-time activity. Once the sources are configured in the Impact analysis dependency update configuration module, the dependency updates are synchronized in the BIA.

For more information on setting up the Impact analysis dependency update configuration module, see Configuring the impact analysis dependency updates.

## Roles associated with BIA dependency updates

Users with the following roles typically check for the dependency updates in a BIA:

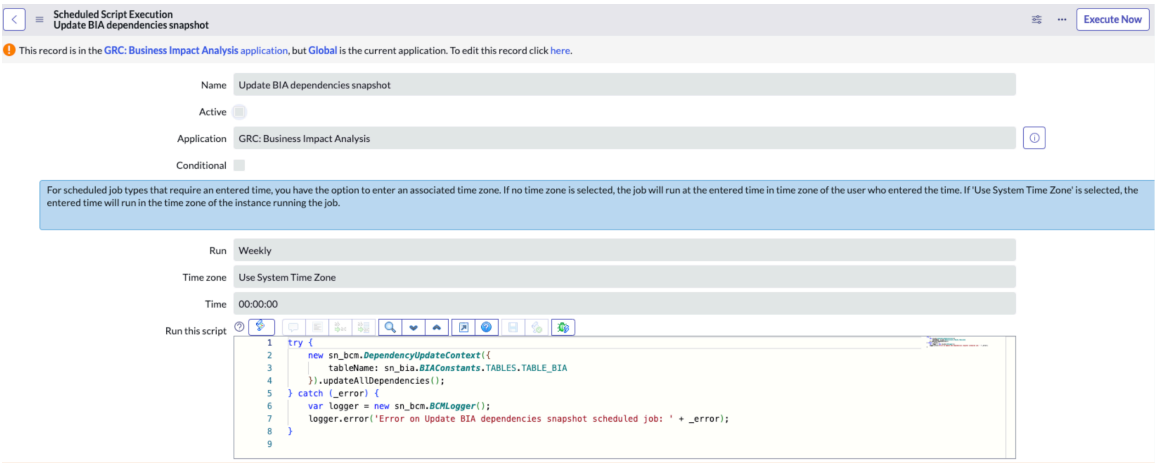
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The BCM program managers, BCM planners, and BCM managers can update the latest dependencies.
- BCM administrators can configure the Impact analysis dependency update configuration module.

A user who can update the dependency assessment can import the dependency updates for a BIA.

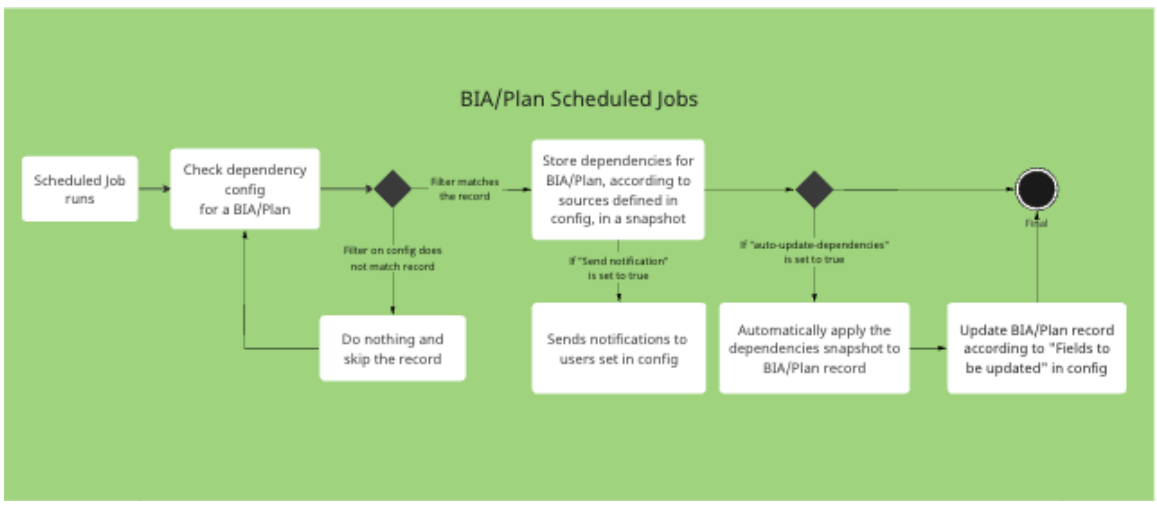
## Using the scheduled job to auto-update the dependencies

The *Update BIA dependencies snapshot* scheduled job is shipped as part of the base system. It runs at regular intervals and fetches the dependency updates. The scheduled job is shown in the following example.




The scheduled job is not marked as Active by default. To run the scheduled job at regular intervals, the system administrators can select the **Active** option and select **Execute now** to set up a schedule. The scheduled job then runs at regular intervals, scans the BIA records for the changes, and fetches the dependency updates for the updated BIA records. It creates a snapshot record for each BIA update.

The scheduled job processes a workflow to check for the changes in the relationships and save the dependency updates automatically as shown in the following example.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. The scheduled job runs weekly, checks the dependency configuration for each BIA record, and fetches the BIA dependencies from CMDB as defined in the **Sources** tab of the Impact analysis dependency update configuration module. It generates a list of all active BIAs and the primary and dependent assets of each BIA. If any new dependencies are added, updated, or deleted for a BIA, the scheduled job creates a snapshot record for the BIA that displays the changes for the user.

   **Note:** By default, the scheduled job checks all the BIA records that are not in the **Archived** state for any updated dependencies.

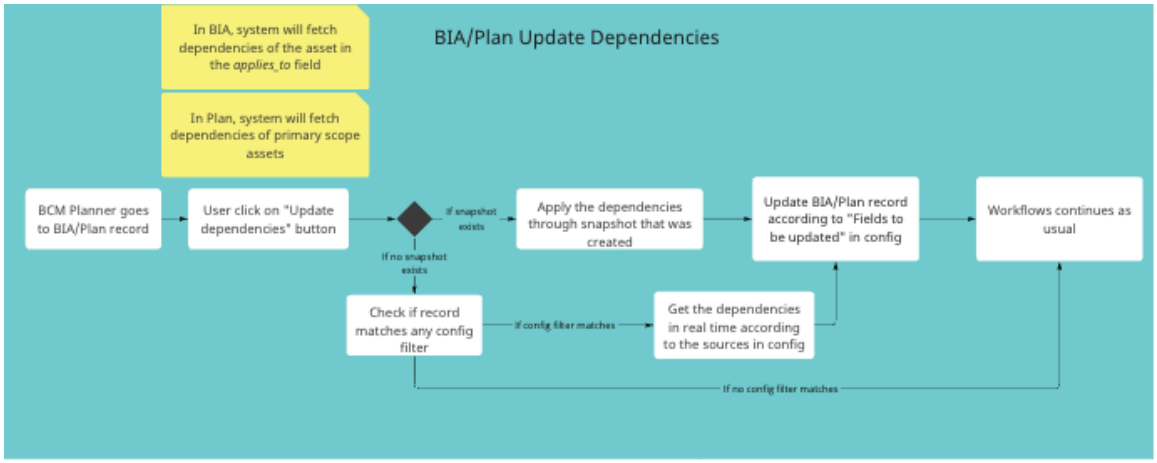
2. The scheduled job refers to the filter condition that is set in the configuration (Impact analysis dependency update configuration module). If the condition matches the BIA record, the scheduled job fetches and stores the dependencies for the BIA in the snapshot record, according to the sources defined in the configuration. If the filter condition does not match the BIA record, the application skips the record.
3. The application combines the assets list into a single list that is based on the priority defined in the Impact analysis dependency update configuration module. The application compares the asset list with the existing asset list and assigns either the **Added**, **Updated**, or **Deleted** state to each asset.
4. The application also compares the new assets to the assets listed in the Element definition and verifies the element definition condition. The application creates a snapshot of the asset and auto-completes the dependency updates in the Dependency snapshot record.
5. When the **Send notification** option is set to **True** in the Impact analysis dependency update configuration module, the users of the BIA record set in the configuration are notified about the dependency updates through the scheduled job.
6. When the **Auto-update dependencies** option is set to **True** in the Impact analysis dependency update configuration module, the scheduled job automatically applies the dependencies snapshot to the BIA record.
7. As the final step, the scheduled job updates the BIA record according to the fields to be updated in the configuration.

## Updating the dependencies manually

As the BCM application user, you can update the BIA dependencies instantaneously by using the **Update dependencies** UI action. In this way, you can update the dependencies manually before the scheduled job runs as per the weekly schedule. The **Update dependencies** UI action is listed in the Dependency assessment of the BIA. The dependencies are then updated in the sources and a snapshot record of the BIA update is created.

See the following workflow for using the **Update dependencies** UI action and updating the dependencies manually:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




1. The BCM planner navigates to a BIA record. The application fetches the dependencies of the asset defined in the **Applies to** field of the BIA.
2. The BCM planner selects the **Update dependencies** UI action that is listed in the Dependency assessment of the BIA.
3. If the snapshot record exists for the BIA update, the system applies the dependencies through the snapshot and updates the BIA according to the **Fields to be updated** in the configuration. The BIA workflow then continues for the next steps such as requesting review and approval.

   If the snapshot record does not exist for the BIA update, the BCM planner checks if the BIA record matches any configuration filter:

   - If the BIA record matches any configuration filter, the application gets the dependencies in real time according to the sources in the configuration. Then, update the BIA record according to the **Fields to be updated** in the configuration. The BIA workflow then continues for the next steps.
   - If the BIA record does not match the configuration filter, the BIA workflow then continues for the next steps.

For more information on updating the dependencies manually, see Update the BIA dependencies manually.

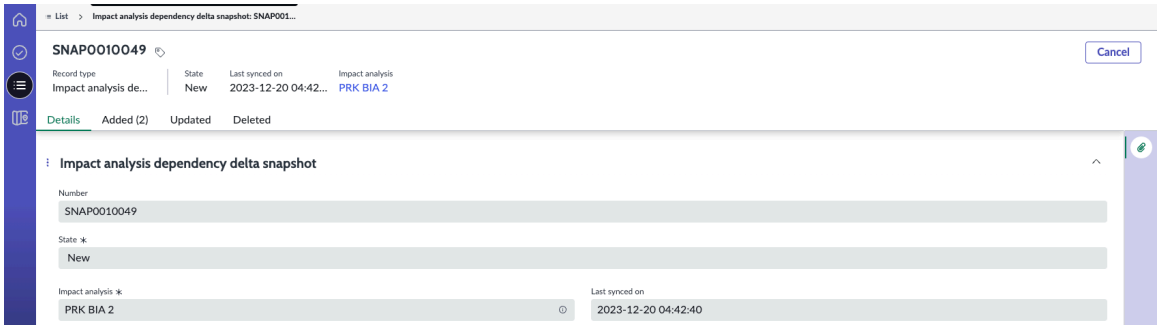
**Note:**

**Note:** The Impact analysis dependency update configuration module is used for using the scheduled job and for updating the dependencies manually (by using the **Update dependencies** UI action).

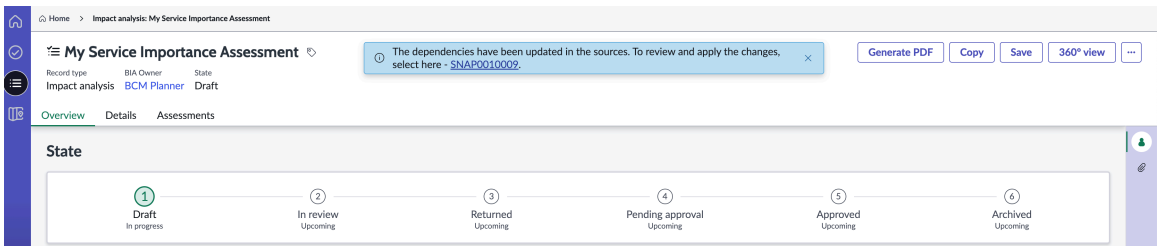
## Snapshot records of the BIA

A snapshot record is created for each BIA update either with the scheduled job or with the **Update dependencies** manual UI action. If any new dependencies are added, updated, or deleted for a BIA, the snapshot record displays the delta of the changes. The snapshot records are listed in the Pending updates module in the Business Impact Analysis list view of the Business Continuity Workspace. A snapshot record is shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




When a snapshot record gets created, the application displays the following UI message in the Dependency assessment of the BIA to inform the users about the dependency updates: `The dependencies have been updated in the sources. To review and apply the changes, select here - <link>`. The UI message is shown in the following example.




The snapshot records are used for record keeping purposes. The BCM application stores one active snapshot for each BIA at a time. Whenever the dependencies are updated, a snapshot is always created first. As the system processes all the records one by one, the snapshot records are auto-committed one by one in the system.

The snapshots that are in the **Completed** state and that have not been updated for a few months are removed from the application automatically.

If the BIA record does not have any changes in the dependencies, then a snapshot record is not created for that BIA record.

## Data Relationships Framework

When you perform a business impact analysis (BIA) on an asset, you must evaluate the dependencies of the BIA by performing a dependency assessment. If the dependencies in the CMDB are updated, importing them manually in a BIA can be a tedious activity. Beginning with the Utah release, the Data Relationships Framework application (com.sn_app_grc_relationship_config) supports the BCM application with the underlying framework to fetch the dependencies in the BIA. The Data Relationships Framework application is installed with the BCM application by default.

For more information on the Data Relationships Framework, see Data Relationships Framework.

### Update the BIA dependencies manually

Update the business impact analysis (BIA) dependencies manually from the snapshot if the scheduled job is not activated in the Impact analysis dependency update configuration module. You can update the dependencies in an active BIA.

**Before you begin**
Role required: sn_bcm.program_manager, sn_bcm.planner, sn_bcm.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

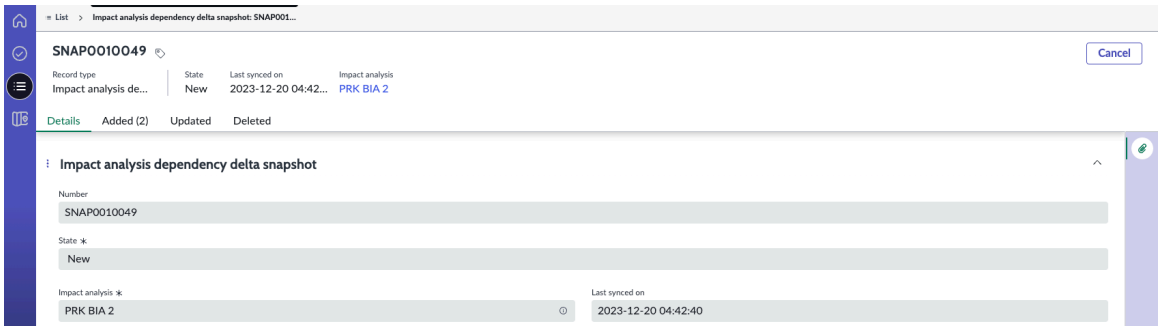
## Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. Open a BIA in the **Draft** state and navigate to the **Assessments** tab.

   If the dependencies have been updated in the sources, the scheduled job fetches the dependencies, and a UI message is displayed on the screen: `To review and apply the changes, select here - SNAP0010078`. You can select the snapshot record to view the updates.

3. To view the snapshot record, select the **Pending updates** module in the **Business Impact Analysis** list view and select a snapshot record.

   The Impact analysis dependency delta snapshot is displayed.




   The BCM application stores one active snapshot for the BIA at a time. The snapshots that are in the **Completed** state and that have not been updated in the past six months are removed from the application automatically.

4. To update the dependencies manually, select **Open assessment** in Dependency assessment.
5. Select **Update dependencies**.

   **Note:** When the system is updating the dependencies, the UI actions on the BIA record are blocked and you cannot proceed further with the BIA states. The user cannot proceed with further states of the BIA unless the system completes importing the dependencies. The dependencies in the Dependency assessment should be completed before the user proceeds with further states of the BIA. Once all the dependencies have been imported and the dependencies in the Dependency assessment are completed, the user can continue with the workflow for the BIA record.

   A UI message is displayed on the screen: `Dependencies are being updated. Refresh the page to view the updated dependencies and complete the assessment.`

6. To save the changes to the BIA, select **Save**.
   The BIA owners and approvers can update the dependencies by saving the changes to the BIA.

### Assess the impact categories and dependencies

Assess the impact categories and dependencies in BCM UIB Workspace to get the necessary information for a plan. Use the business impact analysis to identify the recovery time objective for an item and prioritize the assets that have the least and most critical dependencies. Use the information to establish their recovery strategies during the planning phase.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

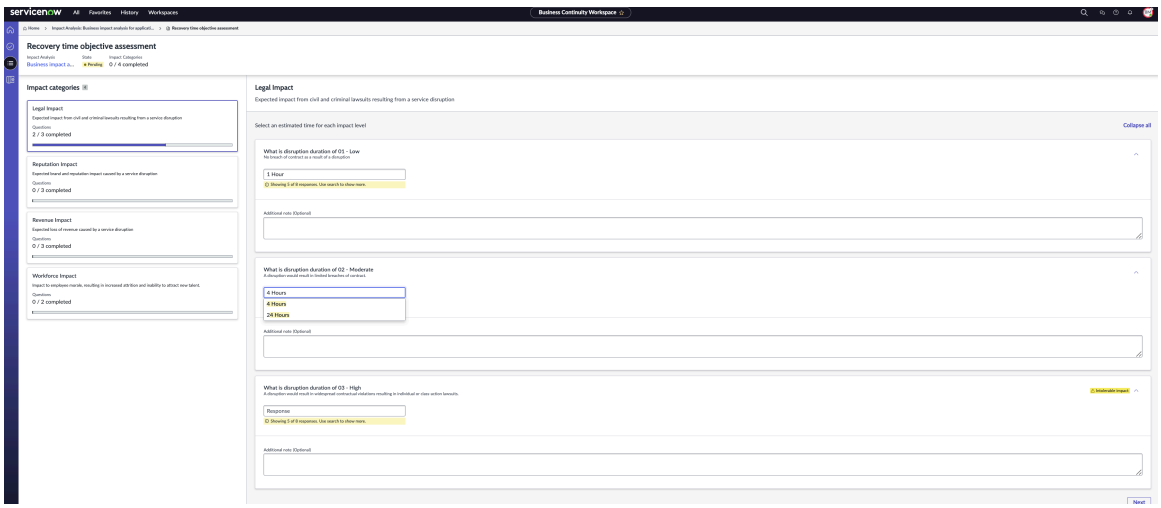
### Before you begin

Role required: sn_bia.bia_admin, sn_bcm.program_manager, sn_bcm.planner

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. To update an existing business impact analysis, select the link to the business impact analysis record in the **Name** column and navigate to the **Assessments** tab.
3. To assess different types of business impact categories on the business process, select the **Recovery time objective assessment** tab.

   A sample questionnaire for the Recovery time objective assessment (RTO assessment) is shown in the following example.

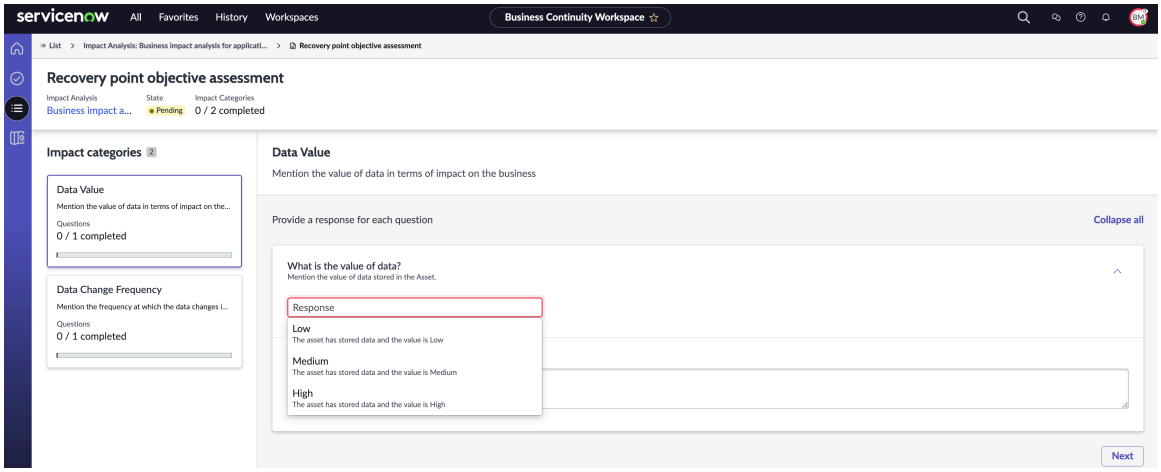



   You must configure all impact categories in the Recovery time objective assessment. A business process draws a set of impact categories, by default, from the template that you have used for the business impact analysis. For more information, see: Review an impact category and assess its downtime.

4. Respond to the questions in the Recovery time objective assessment questionnaire and select **Next**.
   For information on recovery time objective and calculation of recovery time objective, see Recovery time objective, Recovery point objective, and Recovery tiers and Calculating the recovery time objective and recovery point objective.
5. To answer questions related to the data component of the asset, select the **Recovery point objective assessment** tab.

   A sample assessment questionnaire for the Recovery point objective assessment (RPO assessment) is shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



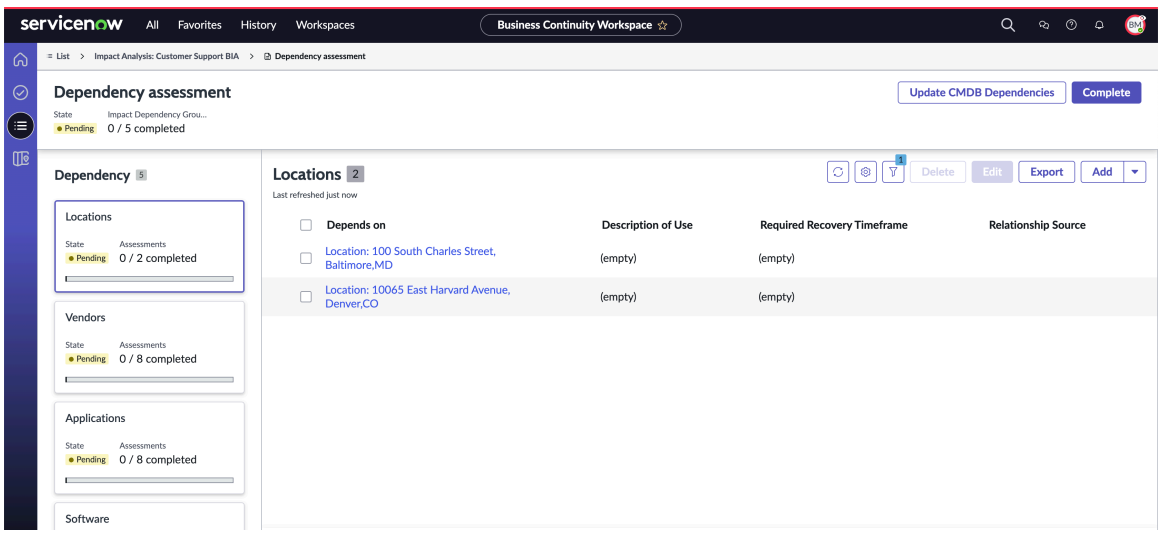

You must configure all impact categories in the Recovery point objective assessment. For more information, see Assess RPO impact of technology assets on the business.

For information on recovery point objective and calculation of recovery point objective, see Recovery time objective, Recovery point objective, and Recovery tiers and Calculating the recovery time objective and recovery point objective.

6. Respond to the questions in the Recovery point objective assessment and select **Next**. You can respond to the questions and complete the Recovery point objective assessment.
7. To assess the dependencies and identify the items within each dependency that your business process depends on, select the **Dependency Assessment** tab.

   You can select the dependency in the Dependency panel to view the group and items that belong to that group. For example, if the group is **Locations**, you can select one or more locations and assess the dependencies associated with them.

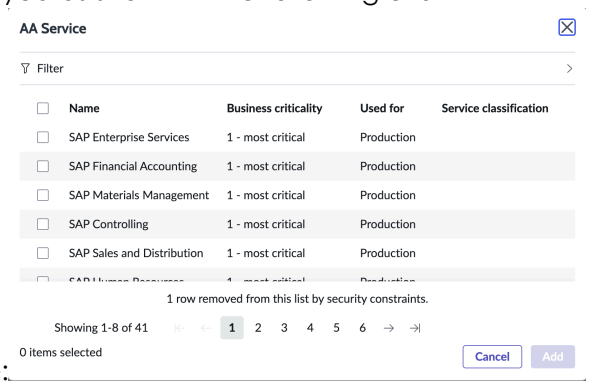
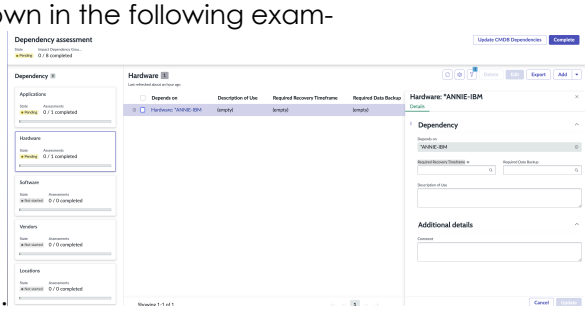
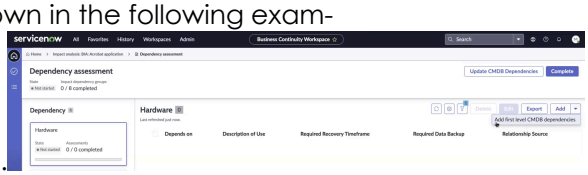
   A sample Dependency assessment questionnaire is shown in the following example.



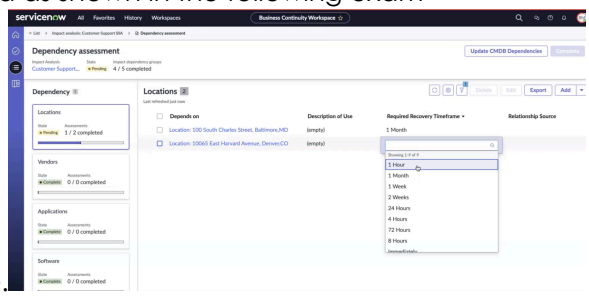
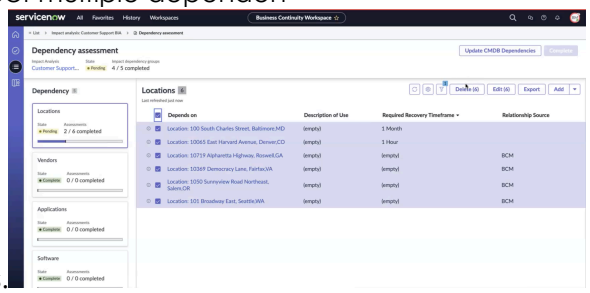
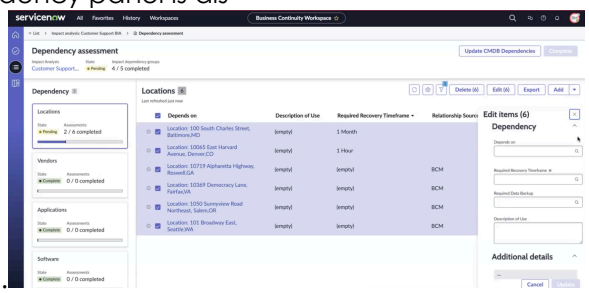
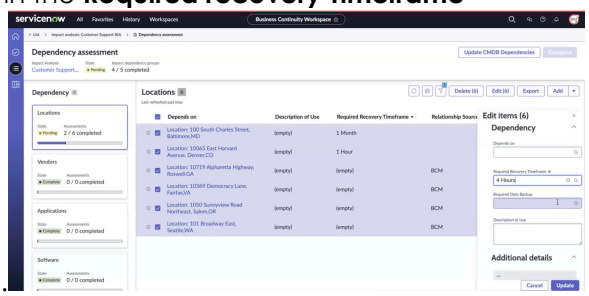

8. To add an item to a dependency group, select one of the following options.

| Step | Description |
| --- | --- |
| **Add** | Add an item from all the records. The relationship source is BCM. All items |

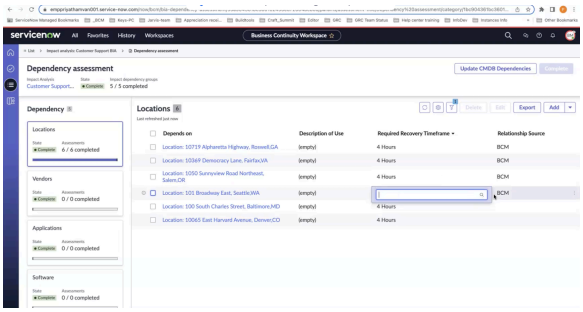
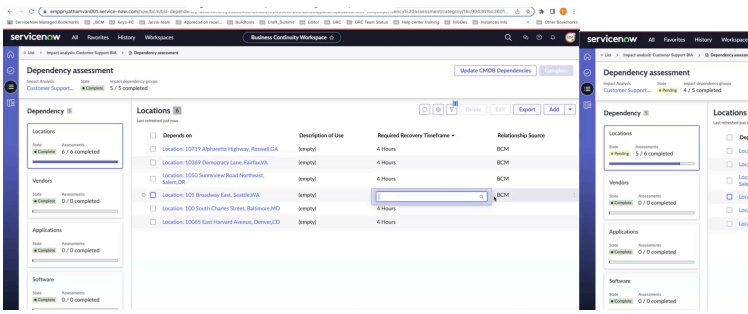
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Step | Description |
| --- | --- |
| | from the respective table, irrespective of its relationship in the CMDB are displayed. When you select **Add**, the filter for selecting the dependencies is displayed as shown in the following example:<br>  <br><br>To update the selected dependency item, you can add the following details and select **Update**.<br>◦ **Depends on**<br>◦ **Required Recovery Timeframe**<br>◦ **Required Data Backup**<br>◦ **Description of Use**<br>◦ **Additional details - Comment**<br>A sample assessment is shown in the following example:<br>  <br> |
| **Add first level CMDB dependencies** | Add dependencies for which the relationships are identified in CMDB.<br>A sample assessment is shown in the following example:<br>  <br> |
| **Update dependencies** | Import all CMDB relationships manually in the respective categories that are defined in the instance. |

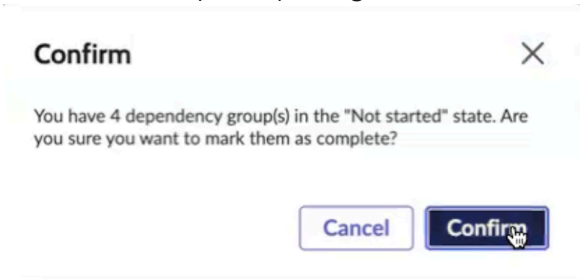
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Step | Description |
| --- | --- |
| Edit **Required Recovery Timeframe** (RTO) for one dependency | If you have one dependency in the **Pending** state, you can update its RTO by updating the inline value in the **Required Recovery Timeframe** field as shown in the following example.<br>  |
| Edit **Required Recovery Timeframe** for multiple dependencies | Similarly, you can update the RTO for multiple dependencies as shown in the following step-by-step examples:<br>**a.** Select multiple dependencies.<br>  <br>**b.** Select **Edit**. The Edit items Dependency panel is displayed.<br>  <br>**c.** Update the RTO for multiple dependencies in the **Required recovery Timeframe** field.<br>  |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

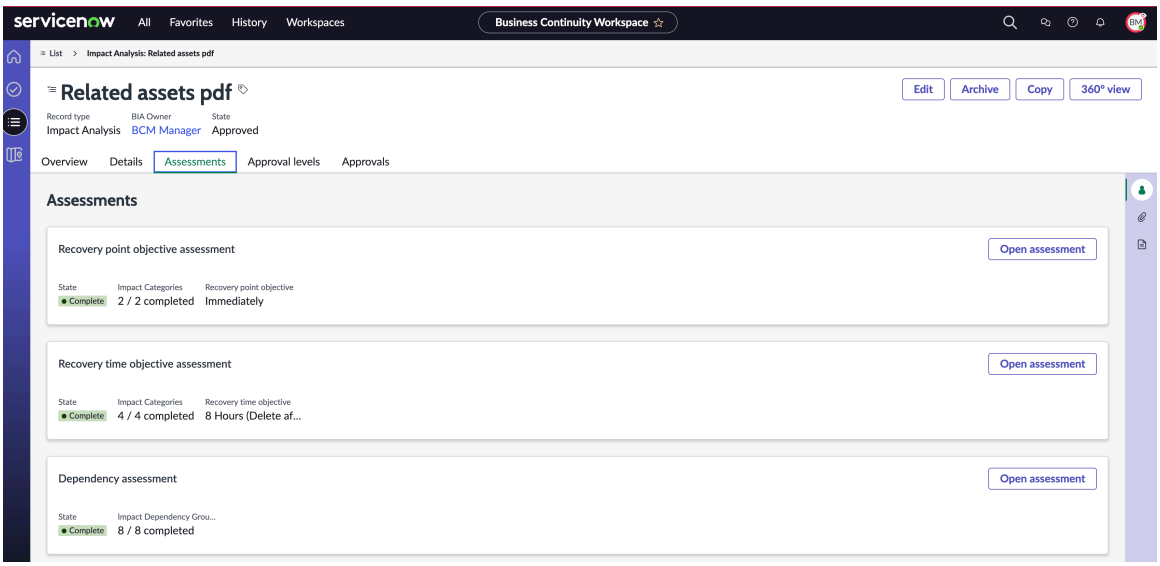
| Step | Description |
| --- | --- |
| | RTO is updated for multiple dependencies and the dependency assessment is marked as Complete.<br>  <br>If you edit the RTO for one dependency, the dependency assessment moves to the **Pending** state.<br>  <br>When you have updated the RTO value for all entries in the **Required Recovery Timeframe** field, then that particular category of dependency is marked as Complete by the application. |
| Select **Complete** | Final step. You must complete all the pending assessments before selecting the **Complete** action button. Selecting **Complete** marks all the assessments in the business impact analysis as Complete. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Step | Description |
| --- | --- |
| | **Note:** After selecting **Complete**, if you see the following message that the dependency groups are in the **Not started** state, you must complete the procedures explained in this table for single and multiple dependencies. Selecting **Confirm** in the following message window marks all dependency groups as Complete without actually completing them.   |

You can prioritize your business continuity and recovery plans based on the criticality of the assets that your business process uses.

The completed assessments are shown in the following example. The state of each assessment is marked as Complete and it is highlighted in Green. You can open the completed assessments and view their details for reference at any time.



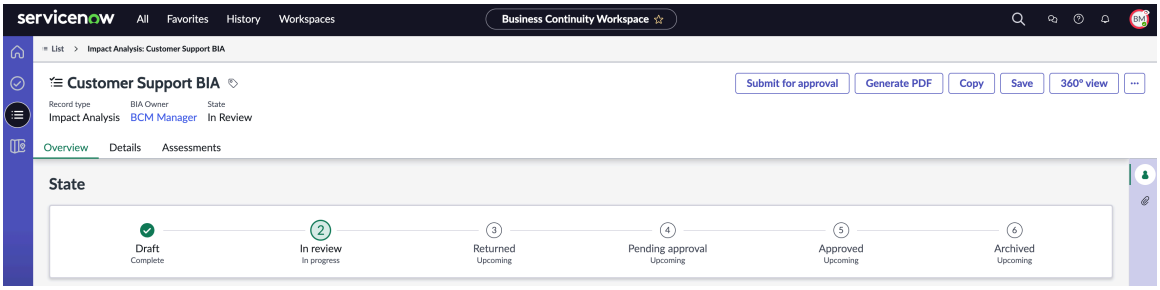

9. Select **Submit for review**.

   **Note:** Before submitting the business impact analysis for a review, ensure that all assessments are complete and the name of the BCM lead is updated in the **BCM Lead** field on the **Details** tab.

   The business impact analysis is submitted for a review to the BIA owner or BCM lead. The business impact analysis is in the **Review** state.

10. Review the assessments in the business impact analysis if you are the BIA owner or BCM lead.

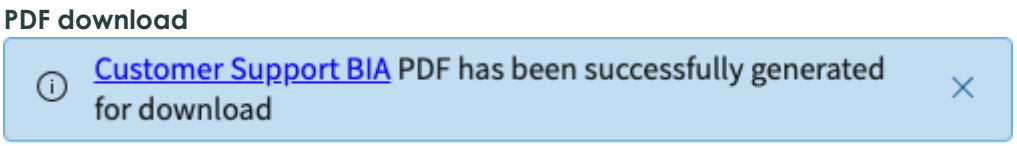
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




11. Select **Submit for approval**.
    The business impact analysis is updated to the **Pending approval** state.

    **Note:** If an approval record is already created for a BIA, the **Approve** or **Reject** buttons are not displayed in the BIA form.

12. Select **Save**.
13. Select the **Generate PDF** button to generate the BIA in a PDF format.
    A message appears that the PDF has been generated.

    Select the link in the message to download the PDF.

    - If you have view-only access to the BIA, the option to generate a PDF helps you to download the document to your local hard drive.
    - You can download the BIA before its **Approval** state.
    - By default, the PDF is generated and attached after the BIA is approved.

14. To move a BIA from **Approved** to **Draft** state, select the **Edit** button.
15. To create a copy of the BIA, select the **Copy** button.
    If you have the permission to read and create a BIA, then you can also copy the BIA.

    a. Enter the name of the new BIA in the Copy impact analysis pop-up.
    The copy action creates an exact replica of the BIA with the name that you enter in the Copy impact analysis pop-up. It also copies all its dependencies and dependency groups on to the new BIA.

    b. Select **Confirm**.

    - The new BIA that is copied from the original BIA has all the RTO, RPO impact, dependency assessment structural details similar to the original BIA.
    - However, the impact category details for each of these assessments are editable for you to assess the dependency details exclusively for the copied BIA.
    - When a BIA that has the RTO or RPO impacted assessments completed is copied, the new copied BIA won't have the new assessment in the **Pending** state. If the impact categories of the RTO and RPO impact assessments in the original BIA are in the **Complete** state, then the impact categories in the copied BIA are in the **Complete** state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Therefore, you must assess and enter the disruption duration, response, and required recovery timeframe relevant to the copied BIA.
- You can assess the details in the **Results** section. The RTO and RPO values are recalculated after you complete the assessments.
- Activities and Work notes are not copied to the new BIA. Enter this information relevant to the new BIA.
- Any attachments attached to the original BIA in any format are copied to the new BIA. However, the PDF generated for the original BIA using the **Generate PDF** button will not be copied over to the new BIA as the assessment data pertain to the original BIA. Since you have the flexibility to modify the assessment details in the copied BIA and generate a PDF, copying the PDF generated for the original BIA has no relevance.

**Note:** You can delete a BIA (and its related tables) that is in the **Draft** state. BCM planner and program manager can delete a BIA that is in the **In Review** and **Returned** states, whereas a BCM admin can delete a BIA irrespective of its state.

### Approve the business impact analysis

Approve the business impact analysis in BCM UI Builder Workspace in the BCM application. If you are the business impact analysis owner or the BCM lead for the business impact analysis, you can approve the business impact analysis.

#### Before you begin

Role required: sn_bia.bia_admin, sn_bcm.program_manager, sn_bcm.planner

#### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. To update an existing business impact analysis, navigate to the business impact analysis record in the **Name** column.
3. Select **Approve** in the form.
   If you are the business impact analysis owner or the BCM lead for the business impact analysis, you can approve the business impact analysis.
   When you approve the business impact analysis, its state is updated to **Approved**.

### Update dependency details of a BIA in Self-Service

Use the contributor role to update the impact category result, RPO Impact analysis responses, state of the impact dependency group, and the work notes in the **Activity** section in the BCM application.

#### Before you begin

Role required: sn_bcm.contributor or sn_bcm.viewer

If you are a BCM contributor and are part of the Contributors list or you are a BCM viewer, then you can update the dependency details of a business impact analysis (BIA).

#### Procedure

1. Navigate to **All** > **Self-Service** > **My Impact Analysis**.
2. View the list of business impact analysis records that are assigned to you and the BIAs that you can contribute to.
3. Select the BIA record and view the details.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Update the **State** of the BIA.
5. To update the record, select **Update**.

### Visualize the 360° relationships for a business impact analysis

Visualize the 360° relationships for a business impact analysis and its associated entities in BCM UIB Workspace. You can access the 360° view at any time while creating a business impact analysis.

## Before you begin

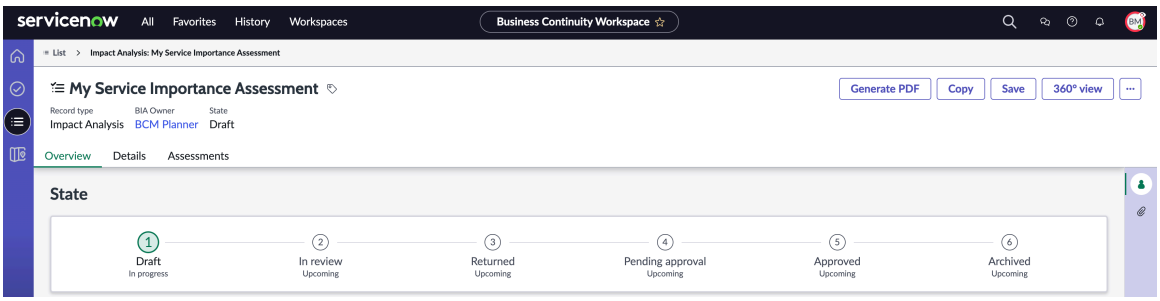
Role required: sn_bia.bia_admin, sn_bcm.program_manager, sn_bcm.planner

## About this task

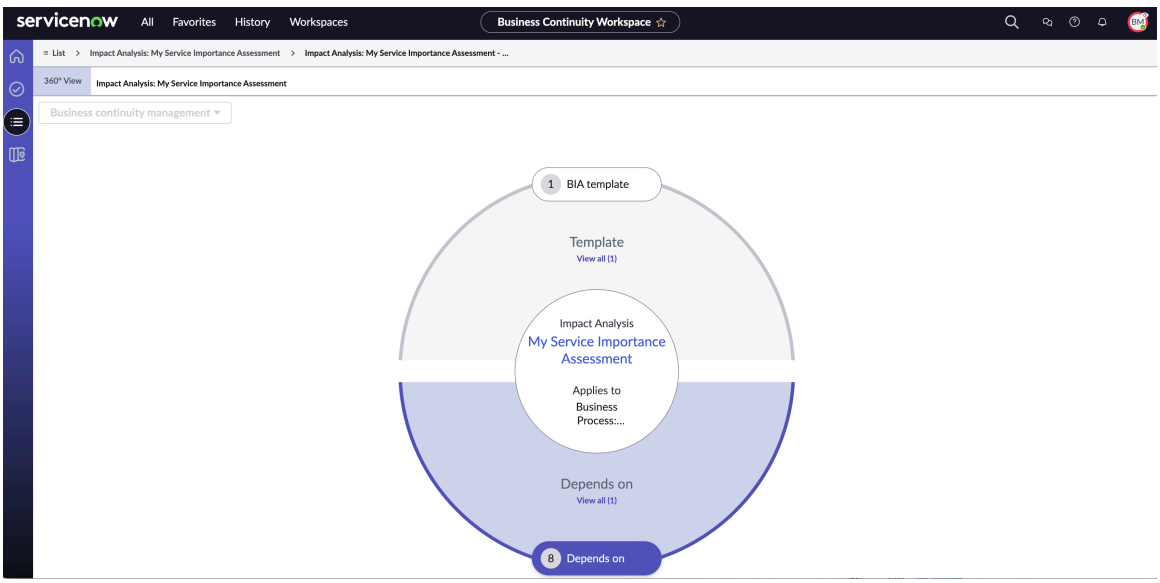
The configurations for the 360° view are stored in **360° View Configurations** > **Configure 360° Views**. If you have the BCM administrator role, you can configure the relationships for the records in **360° View Configurations** > **Relationship Registries**.

## Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Business Impact Analysis** and select a record from the list.
   The business impact analysis record is displayed.
3. Select **360° view**.
   You can select **360° view** to view the relationships for a BIA as shown in the following example.




The following example shows the 360° view of a business impact analysis and its details.



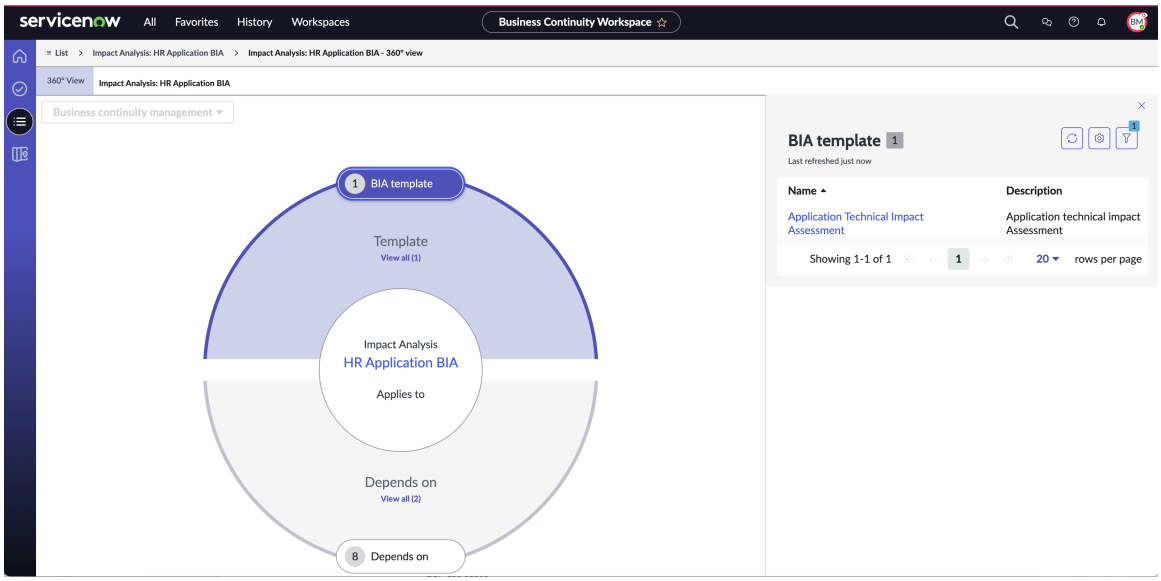

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The 360° view for the business impact analysis shows the following details:

- **Impact Analysis**: Name of the business impact analysis such as My Service Importance Assessment.
- **Applies to**: Entity that the business impact analysis applies to such as Business process or Business service.
- **Template**: BIA template details such as the name of the template and its description. You can select the **BIA template** capsule and view the details of the BIA template.
- **Depends on**: Dependencies associated with the business impact analysis. You can select the **Depends on** capsule and view its details.

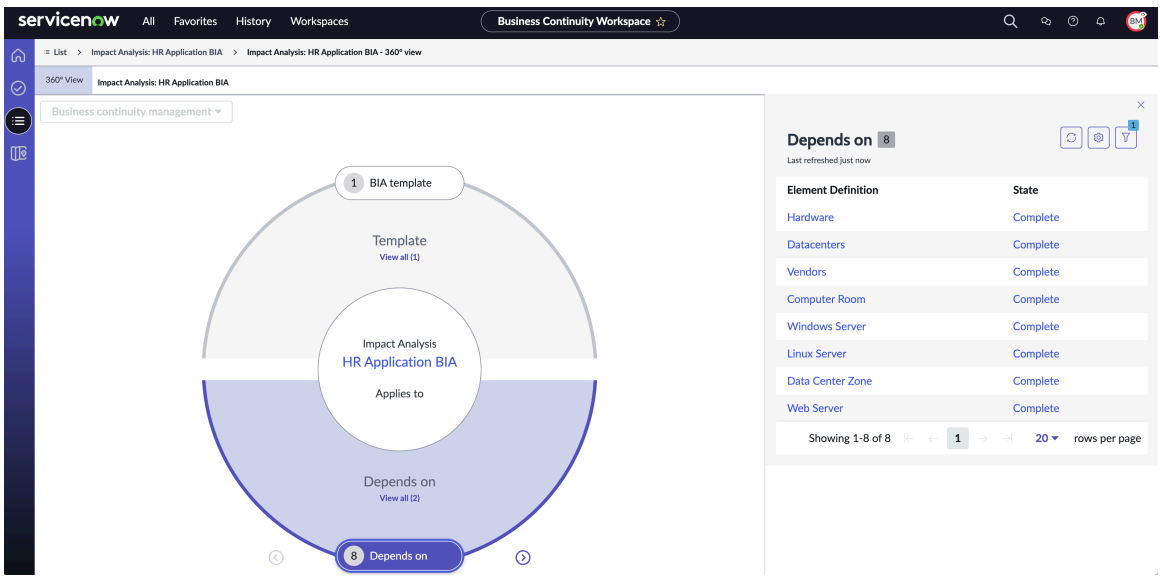
4. Select **BIA template** in the view.

The details of the BIA template such as the name and description of the template are displayed in the right panel of the view as shown in the following example.




5. Select **Depends on** in the view.

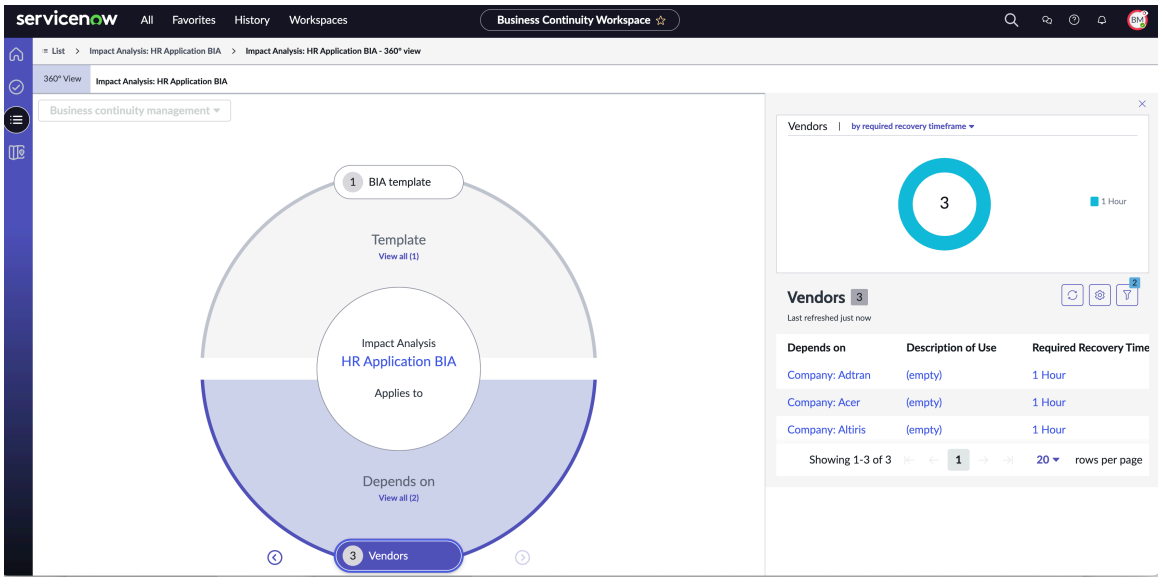
The details of the dependencies are displayed in the right panel of the view as shown in the following example.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Select **Vendors** in the view.

   The details of the vendors are displayed in the right panel of the view as shown in the following example.




7. To navigate to the BIA again, select the BIA or list view in the breadcrumb navigation.

## Generate the PDF of a business impact analysis

Generate a PDF of a business impact analysis in BCM UIB Workspace and save it for a future reference.

### Before you begin

Role required: sn_bcm.program_manager, sn_bcm.planner

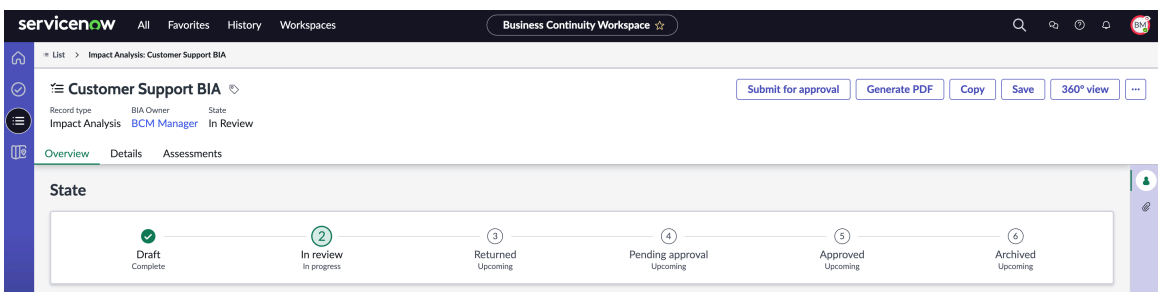
### About this task

To format the PDF for your business needs, see Format the PDF templates for BIA, BCP, and Events.

### Procedure

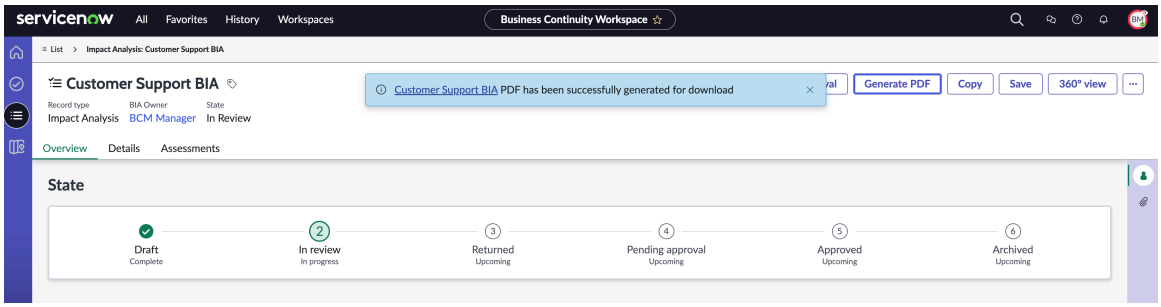
1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Business Impact Analysis** and select any business impact analysis record that is in the **Review** or next state.
3. Select **Generate PDF** in the form.

   The following example shows the **Generate PDF** option in the business impact analysis form.



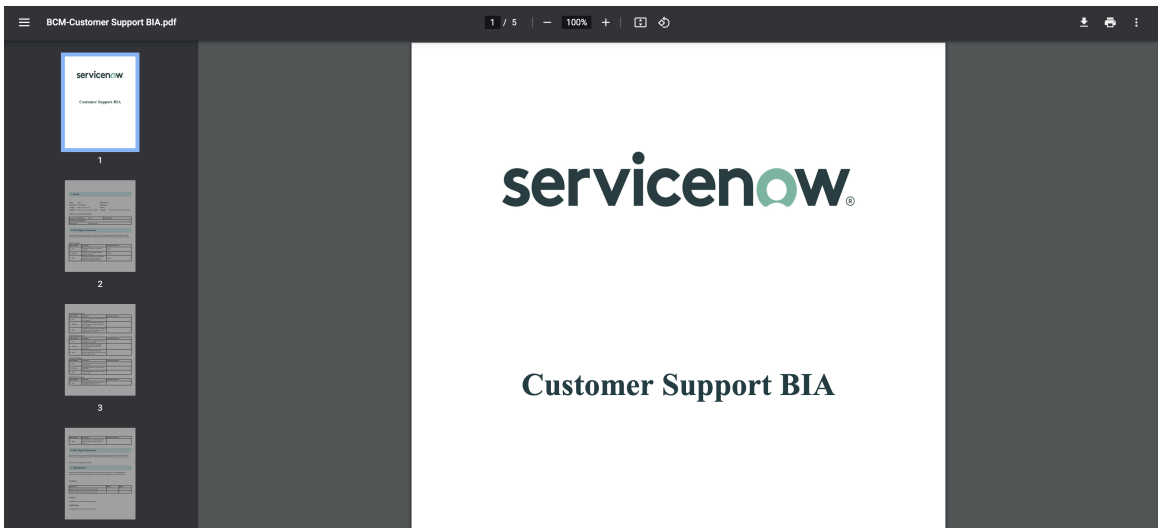

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following example shows the message that is displayed on the screen: `<Name of the BIA> PDF has been successfully generated for download.`




4. To download the PDF, select the link in the message.

   The following example shows the PDF of the business impact analysis.




5. Save the PDF on your system.

## Structured workflows for Business Continuity Planning in BCM UIB Workspace

Perform the structured workflows that are outlined in this section to create a business continuity plan in Business Continuity Workspace (also known as BCM UIB Workspace).

Typically, the business continuity plan owner performs the following tasks:

- Create a business continuity plan as per the plan template. For more information, see Create a business continuity plan.
- Add an asset and scope to the plan. For more information, see Add an asset and scope to the business continuity plan.
- Create a documentation section. For more information, see Create a documentation section.
- Add the related plan and recovery team. For more information, see Add the related plan and recovery team.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Add a loss scenario, recovery strategy, and recovery task. For more information, see Add a loss scenario, Add a recovery strategy for the related asset dependencies, and Add a recovery task for the loss scenario.
- Generate and save the PDF of the analysis for reference. For more information, see Generate the PDF of a business continuity plan.

## Additional information on Business Continuity Planning

- For information on the **Planning** tab in the Home page, see Home page view.
- For information on business continuity planning, see Business continuity planning.
- For information on the administrative tasks in business continuity planning, see Setup for a business continuity plan.

### States and UI actions for a business continuity plan

When you create a business continuity plan, certain UI actions are associated with each state.

## States and UI actions that are associated with a business continuity plan

The states and UI actions that are associated with a business continuity plan are described in the following table.

**UI actions and States associated with a business continuity plan**

| Updated state of the BCP | UI action | Description |
|---|---|---|
| **Draft** | In business continuity plan record Lists view, select **New**.<br><br>**Note:** You can also navigate to the **Planning** section of the Home page and select **Create BIA**. | When you select **New** in the Create New Plan form or **Create BIA** in the Home page, a record is created in the **Draft** state by default.<br><br>On the **Details** tab, add details of the business continuity plan. Add details on the following tabs:<br>• Scope<br>• Documentation<br>• Related plans<br>• Recovery teams<br>• Loss scenarios<br>• Recovery tasks |
| **In review** | Select **Submit for review**. | When you select **Submit for review** in the Create New Plan form, the state of the business continuity plan is updated to **In review**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**UI actions and States associated with a business continuity plan (continued)**

| Updated state of the BCP | UI action | Description |
|---|---|---|
| **Pending approval** | Select **Submit for approval**. | When you select **Submit for approval** in the Create New Plan form, the state of the business continuity plan is updated to **Pending approval**. |
| **Approved** | Select **Approve**. | When you select **Approve** in the Create New Plan form, the state of the business continuity plan is updated to **Approved**. The **Overview** tab displays the progression of the states for the business continuity plan.<br><br>When the business continuity plan is in the **Approved** state, you cannot edit it further. |
| **Archived** | In the Create New Plan form, select **Archive**. | When you select **Archive** in the **Create New Plan** form, the state of the business continuity plan is updated to **Archived**.<br><br>When the business continuity plan is in the **Archived** state, it is available in the read-only format. You can no longer edit the information in these tabs.<br><br>You can perform the following additional UI actions in the Create New Plan form:<br>Generate PDF<br>Download the PDF of the business continuity plan for reference. The PDF attachment is available in the **Activity** panel of the **Details** tab. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**UI actions and States associated with a business continuity plan (continued)**

| Updated state of the BCP | UI action | Description |
|---|---|---|
| | | For more information, see Generate the PDF of a business continuity plan.<br>Copy<br>Save a copy of the PDF of the business impact analysis for future reference as a template.<br>360° view<br>Visualize the 360° representation of the business continuity plan such as its name, scope,related plans, and related tasks.<br>For more information, see Visualize the 360° relationships for a business continuity plan.<br>Delete<br>Delete the continuity plan.<br>Edit<br>Edit the business continuity plan.<br>Save<br>Save the business continuity plan. |
| **Returned** | Select **Reject**. | When the BCP is rejected, it is set to **Returned**. You can edit the business continuity plan in the **Returned** state. |

### Create a business continuity plan

Create a business continuity plan in BCM UIB Workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

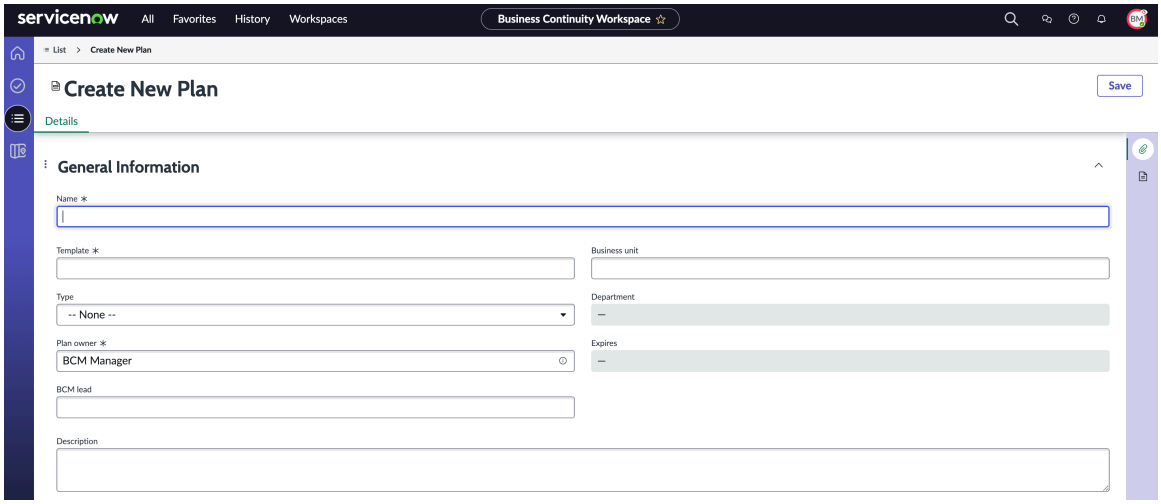
### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Planning** and select **New**.

   The **Create New Plan** form is displayed as shown in the following example.

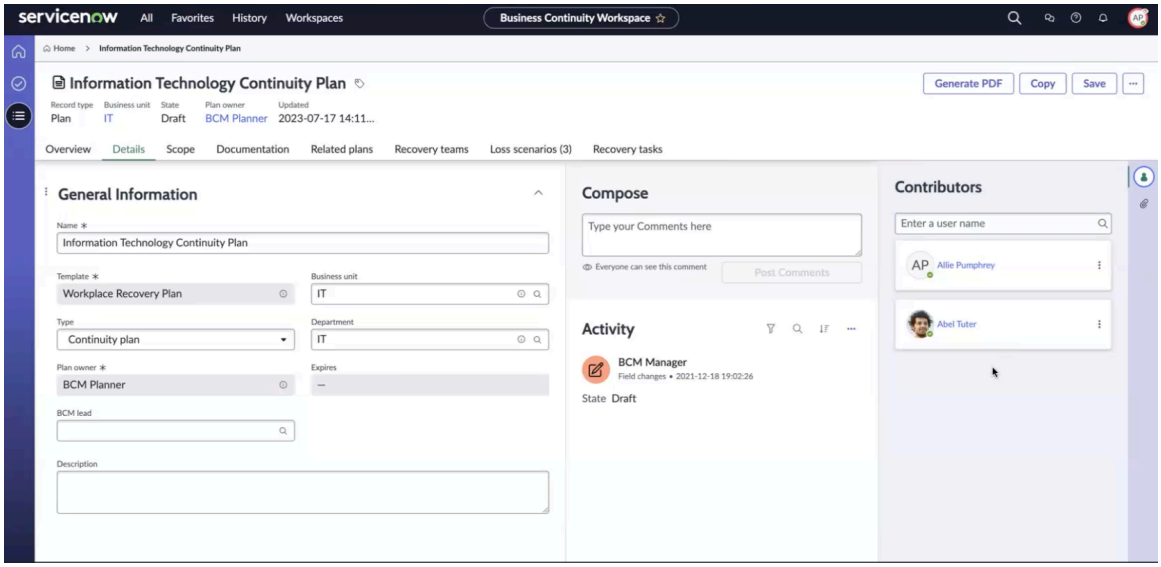



3. In the **Details** tab of the **Create New Plan** form, fill in the required fields.
   For more information on the fields, see Create New Plan form.
   The business continuity plan (BCP) is created in the **Draft** state and it is displayed in the List view. The state and details of the business continuity plan are displayed in the following tabs:
   - **Overview**: You can view the current state and overall state progression of the BCP.
   - **Details**: You can add the details of the plan such as its name, template, type, plan owner, and so on.
   - **Scope**: You can add an asset to the scope of the plan and view the primary elements that are defined in the plan template.
   - **Documentation**: You can document the recovery capabilities of the plan in the documentation sections.
   - **Related plans**: You can add the related plans that are listed in the Workspace view.
   - **Recovery teams**: You can create the recovery teams for the business continuity plan.
   - **Loss scenarios**: You can add the loss scenarios that are applicable to the business continuity plan.
   - **Recovery tasks**: You can create the recovery tasks for the business continuity plan.
4. Launch the **Contributors** panel by selecting the **Contributors** icon in the side-bar and add a contributor from the list to the business continuity plan record.

   The BCP contributors with the sn_bcp.plan_contributor role have read, write, and delete access to the business continuity plan. If you have the BCP manager, BCM lead, or plan contributor role, you can add or remove the contributors.

   The BCP contributors can edit the list of the contributors and edit the BCP as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




5. Select **Save**.
   The BCP is saved in the **Draft** state and it is displayed in the List view of the Planning records.

### Create New Plan form

Use the Create New Plan form in BCM UIB Workspace to add the details about the business continuity plan (BCP).

## Create New Plan form

For a description of the field values, see the following table.

**Create New Plan form**

| Field | Description |
|---|---|
| Overview tab | |
| State | Stepper component that displays the states of the business continuity plan. |
| Details tab | |
| Name | Name of the business continuity plan. You can describe the BCP within 255 characters length. |
| Template | Template that you can use as a model to create the BCP.<br><br>The template BIA has the primary elements (applications, business processes, and locations), impact categories, and the dependent assets identified for the type of assessment. |
| Type | Type of the business continuity plan. Available options are:<br>• Continuity plan<br>• Recovery plan<br>• Crisis response plan |
| Business unit | Business unit that the business continuity plan is created for. Available options are: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Plan form (continued)**

| Field | Description |
|---|---|
| | • Finance<br>• HR<br>• IT<br>• Legal<br>• Marketing<br>• Sales |
| Department | Department related to the business unit. You can select the department based on the business unit selected. |
| Plan owner | Owner of the business continuity plan. |
| Expires | Read-only field. Expiration date for the plan. |
| BCM lead | BCM lead for the business continuity plan. |
| Description | Description of the business continuity plan. |
| Icons displayed in the side-bar of the record | |
| Contributors | Icon to populate side-panel in the record. You can add contributors to the business continuity plan from the panel. |
| Attachment | Panel where the PDF of the business continuity plan is attached. |
| Template | Panel to populate the template for the business continuity plan. You can view all or customized templates in this panel. |

### Schedule an auto-update of the related assets in the plans

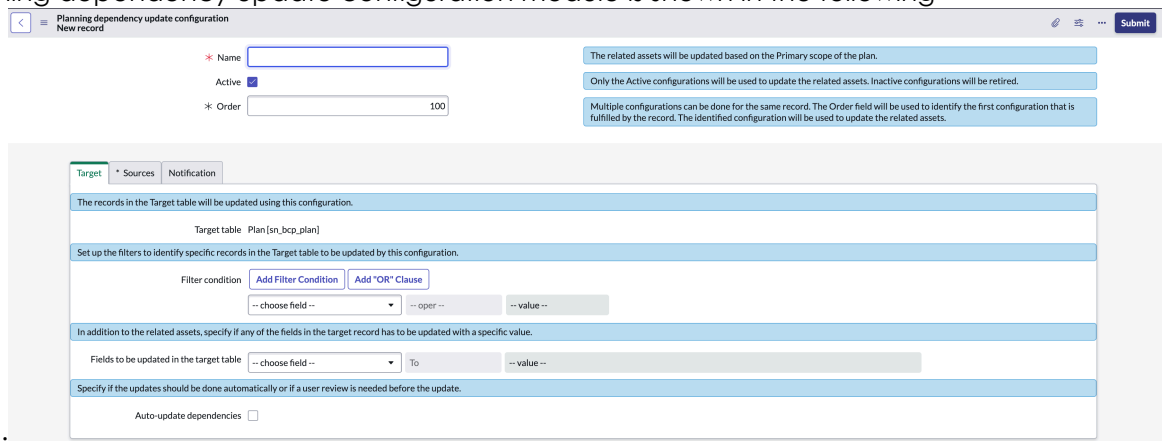
You can schedule an auto-update of the related assets in the plans based on the source data and relationships in the CMDB. You can receive an email notification with details of the plan dependency updates from the BCM application. Dependencies are fetched from different sources such as BIA upstream dependency, BIA downstream dependencies, and CMDB.

## Scheduling an auto-update of the related assets

The BCM administrators can schedule an auto-update of the related assets in the plans in the Planning dependency update configuration module, based on the source data and relationships in the CMDB.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Planning dependency update configuration module is shown in the following example.




When the BCM administrators select the **Auto-update dependencies** option, the BCM application schedules an auto-update of the related assets in the plans. Similarly, when the **Send notification** option is selected, the BCM application sends automated emails to the plan owners about the dependency updates.

Planning dependencies are fetched from different sources such as BIA upstream dependency, BIA downstream dependencies, and CMDB.

**Note:** In the plans, the dependencies are fetched for all primary scope assets.

Setting up the Planning dependency update configuration module is a one-time activity. Once the sources are configured in the Planning dependency update configuration module, the updates are synchronized in the plan.

For more information on setting up the Planning dependency update configuration module, see Configuring the planning dependency updates.

## Roles associated with the auto-update of the related assets in the plans

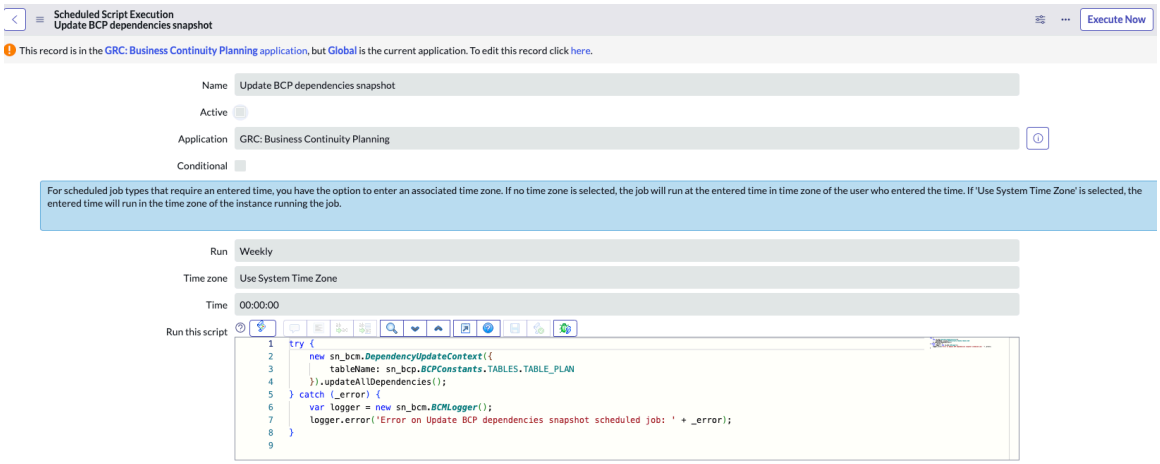
Users with the following roles typically update the related assets in the plans:

- The BCM program managers, BCM planners, and BCM managers can update the related assets in the plans.
- BCM administrators can configure the Planning dependency update configuration module.

## Using the scheduled job to auto-update the dependencies

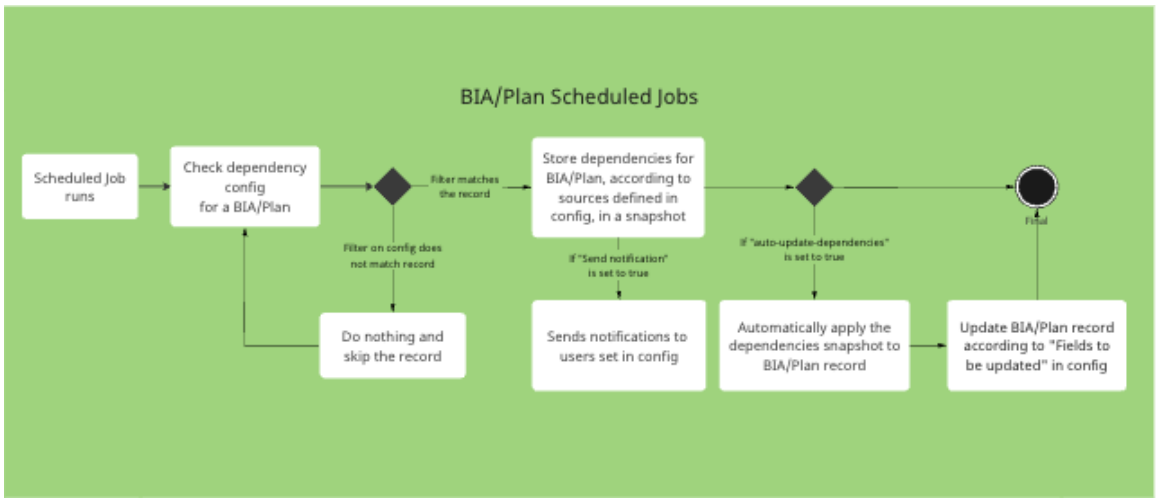
The *Update BCP dependencies snapshot* scheduled job is shipped as part of the base system. It runs at regular intervals and fetches the updated related assets in the plans. The scheduled job is shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The scheduled job is not marked as Active by default. To run the scheduled job at regular intervals, the system administrators can select the **Active** option and select **Execute now** to set up a schedule. The scheduled job then runs at regular intervals, scans the plan records for the changes, and fetches the updated related assets for the planning records. It creates a snapshot record for each planning record update.

The scheduled job processes a workflow to check for the changes in the relationships and save the dependency updates automatically as shown in the following example.




1. The scheduled job runs weekly, checks the related assets configuration for each planning record, and fetches the related assets from the sources defined in the **Sources** tab of the Planning dependency update configuration module.
2. The scheduled job refers to the filter condition that is set in the configuration (Planning dependency update configuration module). If the condition matches the planning record, the scheduled job fetches and stores the related assets for the plan in the snapshot record, according to the sources defined in the configuration. If the filter condition does not match the planning record, the application skips the record.
3. When the **Send notification** option is set to **True** in the Planning dependency update configuration module, the users of the planning record set in the configuration are notified about the updated related assets through the scheduled job.

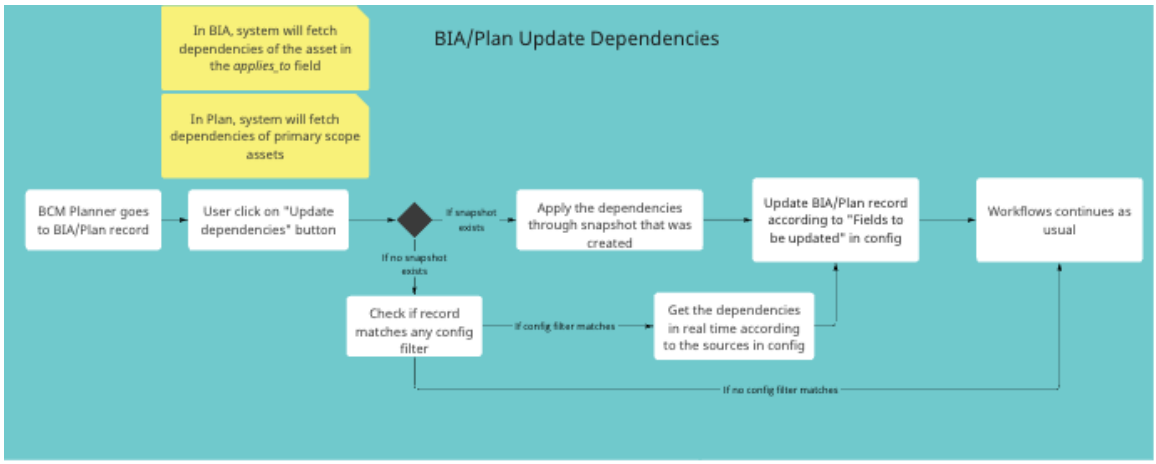
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. When the **Auto-update dependencies** option is set to **True** in the Planning dependency update configuration module, the scheduled job automatically applies the Plan dependency snapshot to the planning record.
5. As the final step, the scheduled job updates the planning record according to the fields to be updated in the configuration.

## Updating the dependencies manually

As the BCM application user, you can update the plan dependencies instantaneously by using the **Update dependencies** UI action. In this way, you can update the dependencies manually before the scheduled job runs as per the weekly schedule. The dependencies are then updated in the sources and a snapshot record of the planning record update is created.

See the following workflow for using the **Update dependencies** UI action and updating the planning dependencies manually:




1. The BCM planner navigates to the planning record. The application fetches the dependencies of the primary scope assets defined in the plan.
2. The BCM planner selects the **Update dependencies** UI action.
3. If the snapshot record exists for the update, the BCM planner applies the planning dependencies through the snapshot and updates the plan according to the **Fields to be updated** in the configuration. The plan workflow then continues for the next steps such as requesting review and approval.

   If the snapshot record does not exist for the update, the BCM planner checks if the planning record matches any configuration filter:

   - If the planning record matches any configuration filter, the application gets the dependencies in real time according to the sources in the configuration. Then, the BCM planner updates the planning record according to the **Fields to be updated** in the configuration. The plan workflow then continues for the next steps.
   - If the planning record does not match the configuration filter, the plan workflow then continues for the next steps.

For more information on updating the planning dependencies manually, see Update the planning dependencies manually.

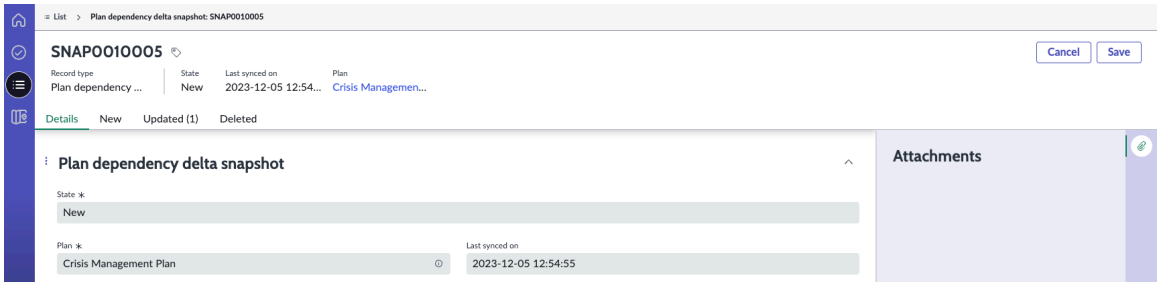
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:**

**Note:** The Planning dependency update configuration module is used for using the scheduled job and for updating the planning dependencies manually (by using the **Update dependencies** UI action).

## Snapshot record of the plan

When the scheduled job runs at set intervals, it creates a snapshot record of each plan update in the application. The snapshot record contains the delta of the changes in the configuration such as new, updated, and deleted assets for the plan. The snapshot records are listed in the Pending updates module in the Planning list view in the Business Continuity Workspace. A snapshot record is shown in the following example.




When a snapshot record gets created, the application displays a UI message to inform the users about the planning dependency updates. The BCM application stores one active snapshot for a plan at a time. The snapshots that are in the **Completed** state and that have not been updated in six months are removed from the application automatically.

If the planning record does not have any changes in the dependencies, then a snapshot record is not created for that planning record.

## Data Relationships Framework

When you create a business continuity plan, you must update the related assets in the plans. Beginning with the Utah release, the Data Relationships Framework (com.sn_app_grc_relationship_config) application supports the BCM application with the underlying framework to fetch the related assets in the plans. The Data Relationships Framework application is installed with the BCM application by default.

For more information on the Data Relationships Framework, see Data Relationships Framework.

### Update the planning dependencies manually

Update the plan dependencies manually from the snapshot if the scheduled job is not activated in the Planning dependency update configuration module. You can update the dependencies in an active plan.

**Before you begin**
Role required: sn_bcm.program_manager, sn_bcm.planner, sn_bcm.admin

**Procedure**

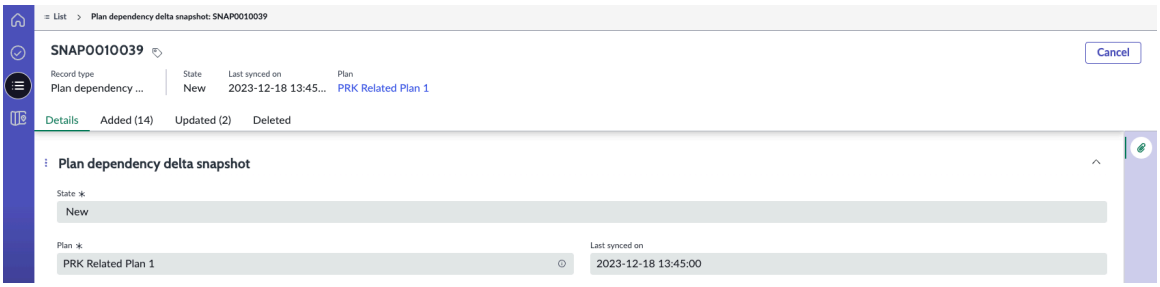
1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. Open a BCP in the **Draft** state and navigate to the **Scope** tab.

   If the dependencies have been updated in the sources, the scheduled job fetches the dependencies. You can select the snapshot record to view the updates.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. To view the snapshot record, select the **Pending updates** module in the **Planning** list view and select a snapshot record.

   The Plan dependency delta snapshot is displayed.




   The BCM application stores one active snapshot for the BCP at a time. The snapshots that are in the **Completed** state and that have not been updated in the past six months are removed from the application automatically.

4. To update the dependencies manually, navigate to the plan and select **Update dependencies**.
   A UI message is displayed on the screen: `Dependencies are being updated.`
5. To save the changes to the plan, select **Save**.
   The plan owners and BCM lead can update the planning dependencies by saving the changes to the plan.

### Add an asset and scope to the business continuity plan

Add an asset and the scope to the business continuity plan. You can then view the primary elements in BCM UIB Workspace.

#### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

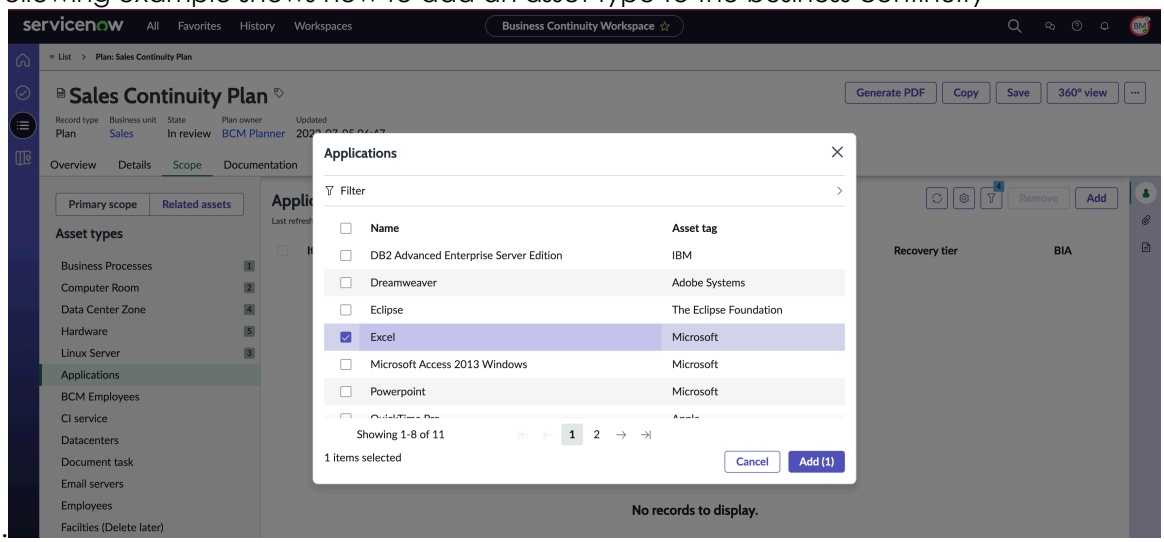
#### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Planning** and select the link to the plan record in the **Name** column.
3. Select the **Primary scope** tab and add primary scope for the business continuity plan.
   If the plan is created from a plan template, you can view the primary elements defined in the plan template.
4. Select the **Related assets** tab and select **Add**.
   The primary elements are listed as Asset types. Assets that are displayed in the **Add Items** modal belong to the element definition type identified in the **Primary element recovered** field of the plan template. You can associate an asset type to the business continuity plan from the following options:
   - Applications
   - Business Processes
   - Computer Room
   - Datacenter Zone
   - Datacenters
   - Employees

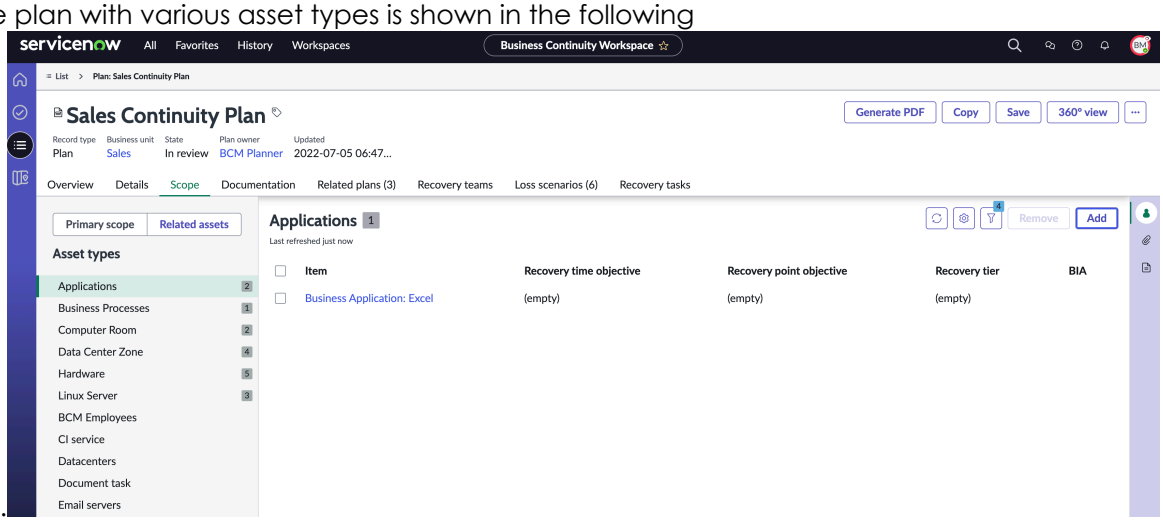
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Hardware
- Linux Server
- Locations
- Software
- Vendors
- Web Server
- Windows Server

The following example shows how to add an asset type to the business continuity plan.




A sample plan with various asset types is shown in the following example.




5. Select **Save**.

## Create a documentation section

Create a documentation section in the business continuity plan. You can then document the recovery capabilities of your business continuity plan in BCM UIB Workspace.

### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

### About this task

The following UI actions are available for the documentation sections:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Update**: Update an existing documentation section.
- **Delete**: Delete an existing documentation section.
- **Reset to template**: Reset an existing documentation section to the Documentation Sections template. You can view the available templates by navigating to **Documentation Sections** of **Business Continuity** in the application navigator. For an existing documentation section, the **Update**, **Delete**, and **Reset to template** actions are available. For a new documentation section, the **Reset to template** action is not available.

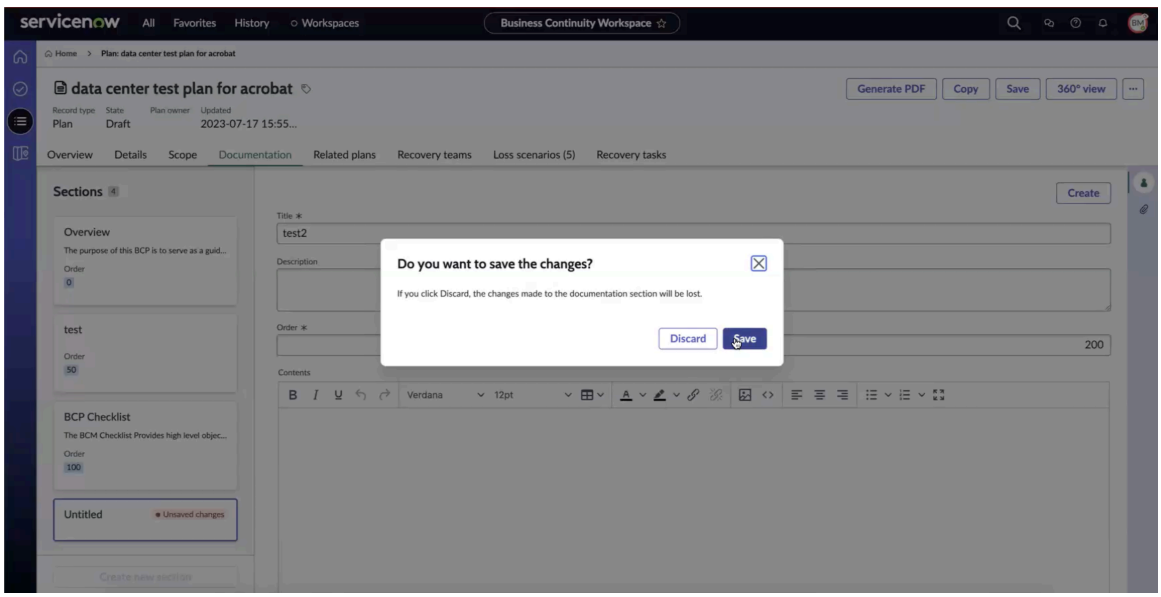
> **Note:** When you create a documentation section on the **Documentation** tab without using the plan template, the **Reset to template** UI action is not available for that documentation section.

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Planning** and select the link to the plan record in the **Name** column.
3. Select the **Documentation** tab of the plan.
4. Select **Create new section**.

   You can add a documentation section in the business continuity plan.

   If you create a documentation section and move away without saving the changes, the documentation section is marked as **Untitled** with the **Unsaved changes** tag as shown in the following example. The following message is displayed on the screen: `Do you want to save the changes?`

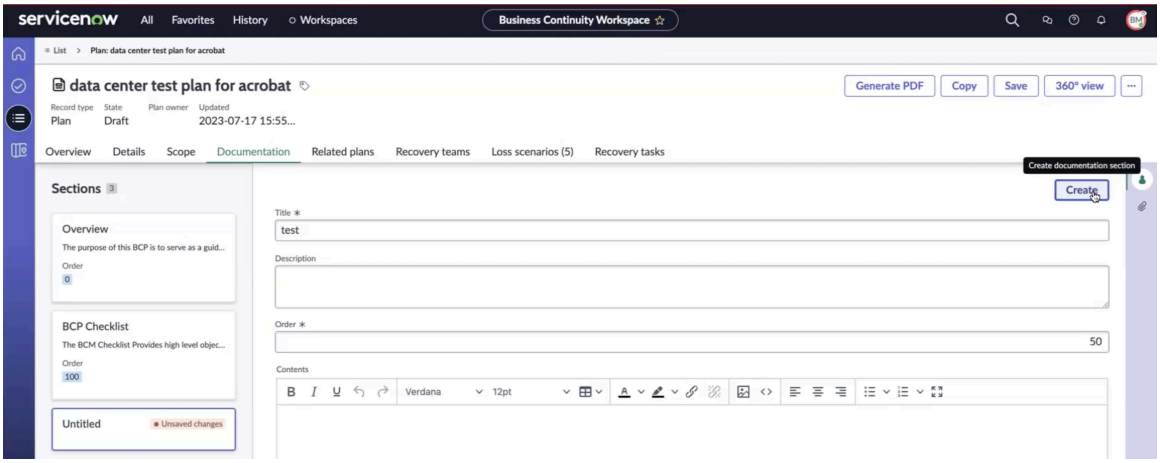



   If you select **Save**, the documentation section is saved in the plan. If you select **Discard**, the changes to the documentation section are not saved.

5. To create a documentation section, select **Create**.

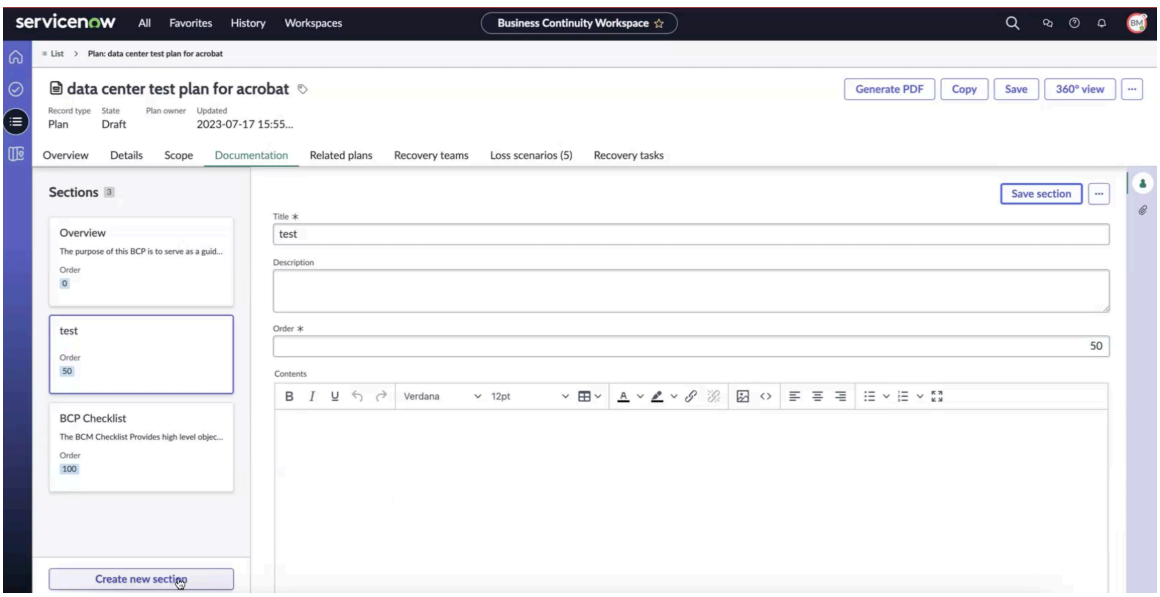
   The following example shows the Overview and BCP Checklist documentation sections in a business continuity plan. The Overview documentation section has an order value of 0. The BCP Checklist documentation section has an order value of 100.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




To create a documentation section that is displayed as the second section in the Sections panel, assign it an order value that is more than 0 and less than 100, such as 50.

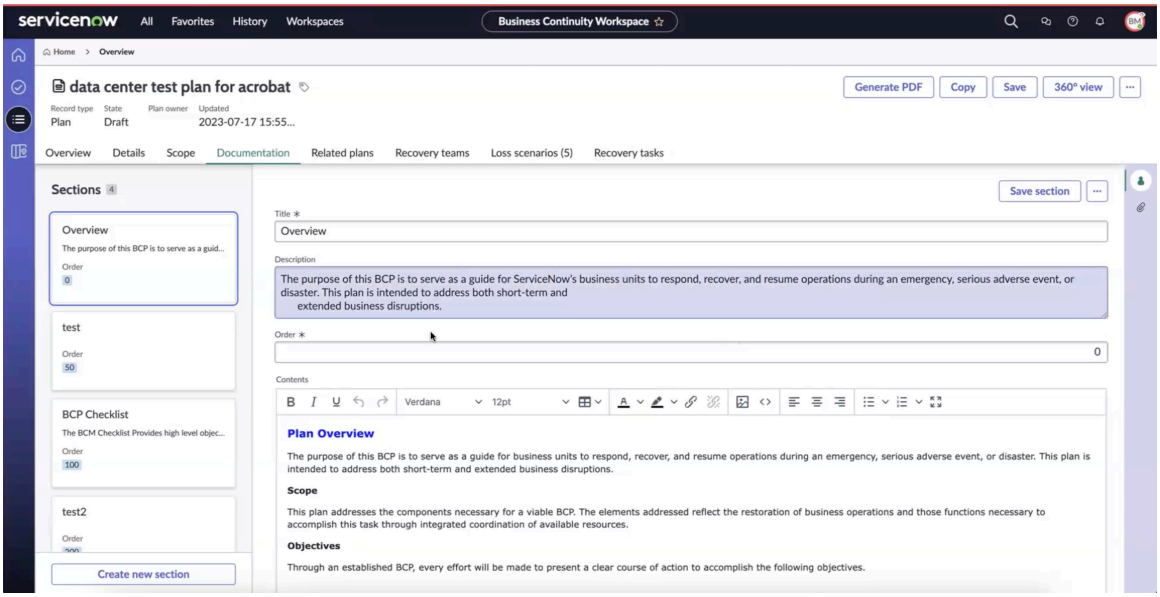
The documentation section with an order value of 50 is displayed as the second documentation section in the Sections panel on the **Documentation** tab.




6. To save the documentation section in the plan, select **Save section**.

   The documentation section is saved in the business continuity plan.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




7. To delete a documentation section in the plan, select **Delete**.
8. To reset a documentation section to its template, select the More actions (**...**) icon and then select **Reset to template**.

## Add the related plan and recovery team

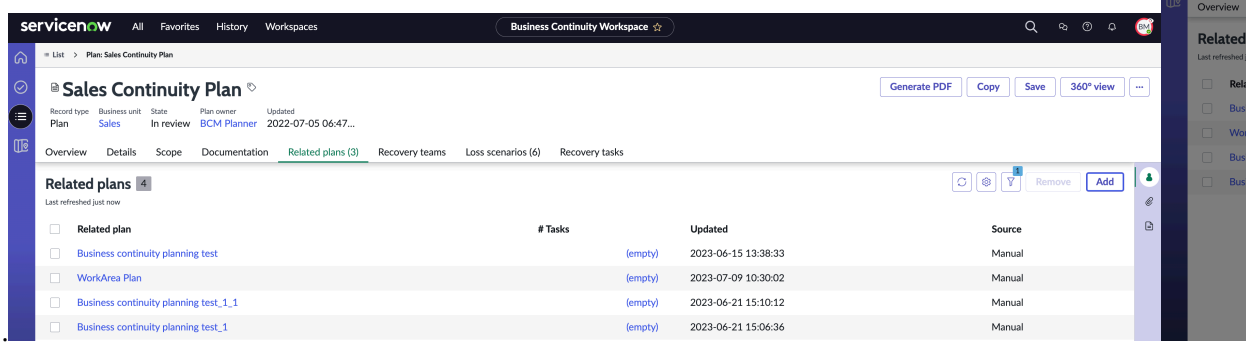
Add your business continuity related plans and recovery teams to your business continuity plan. You can then view the details in BCM UIB Workspace.

### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

### Procedure

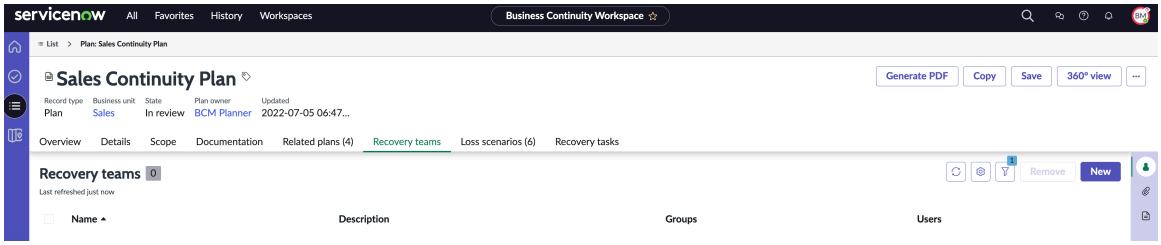
1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Planning** and select the link to the plan record in the **Name** column.
3. Select the **Related plans** tab and select **New**.
   You can add a business continuity related plan as shown in the following examples.

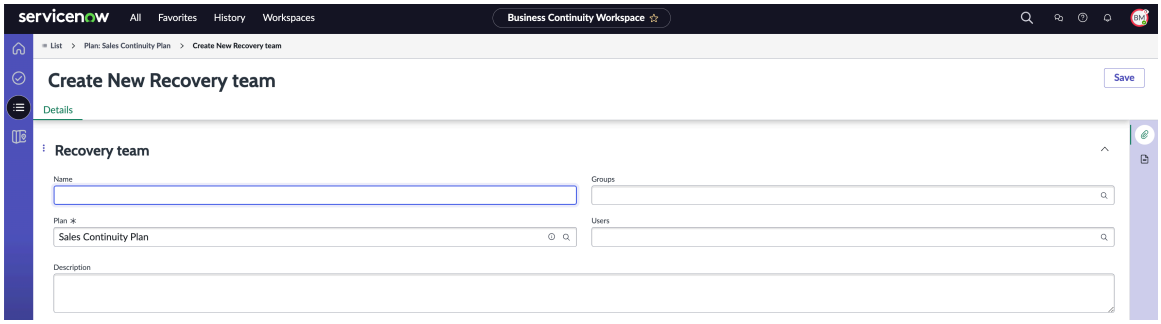



4. Select the **Recovery teams** tab and select **New**.

   You can add a recovery team to the plan as shown in the following examples.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




.

5. Select **Save**.
   The related plan and recovery team are added to the business continuity plan.

## Add a loss scenario

Add a loss scenario and define the related asset dependencies in your business continuity plan. You can then view the details of the assets in BCM UIB Workspace and then plan a recovery strategy for an identified loss scenario.

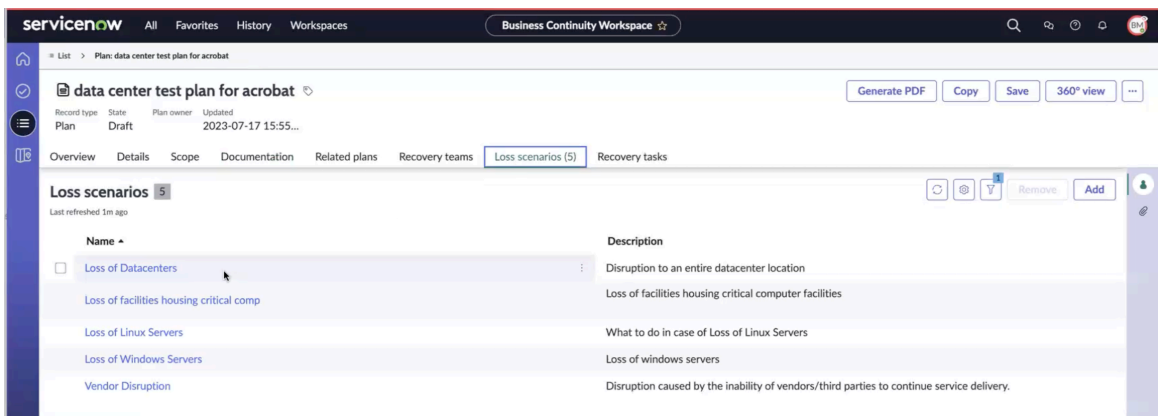
### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

### Procedure

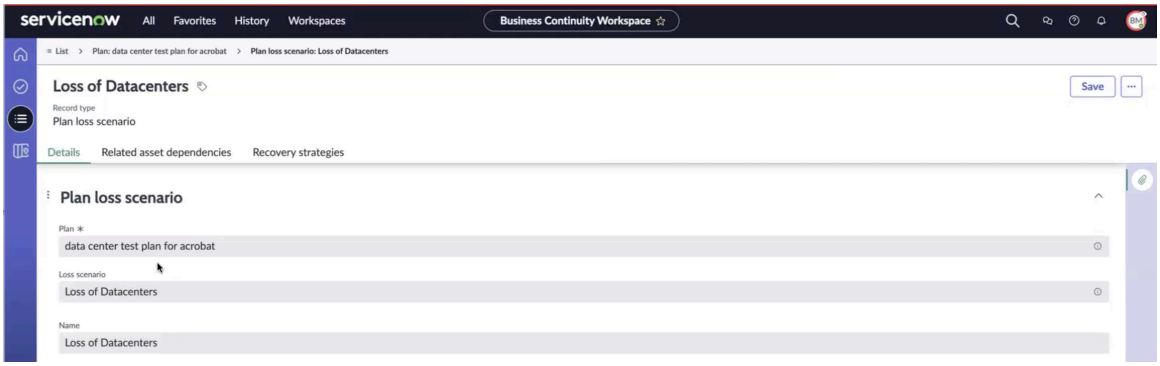
1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Planning** and select the link to the plan record in the **Name** column.
3. Select the **Loss scenarios** tab and select **Add**.

   You can add a loss scenario to the business continuity plan. In the following example, you can select the Loss of Datacenters loss scenario and add it to the business continuity plan.

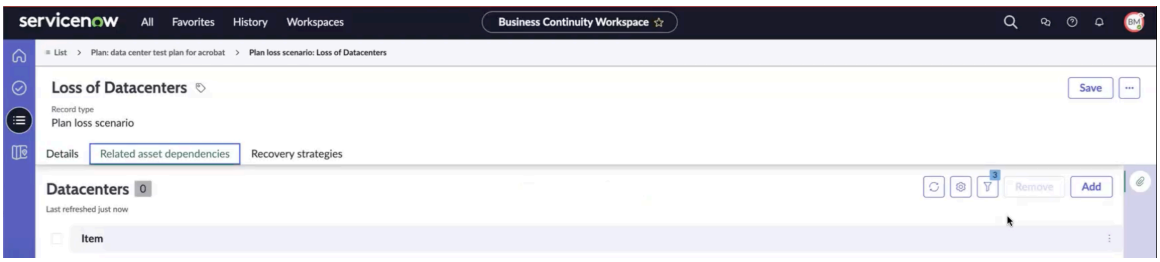



   The loss of scenario record is displayed as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

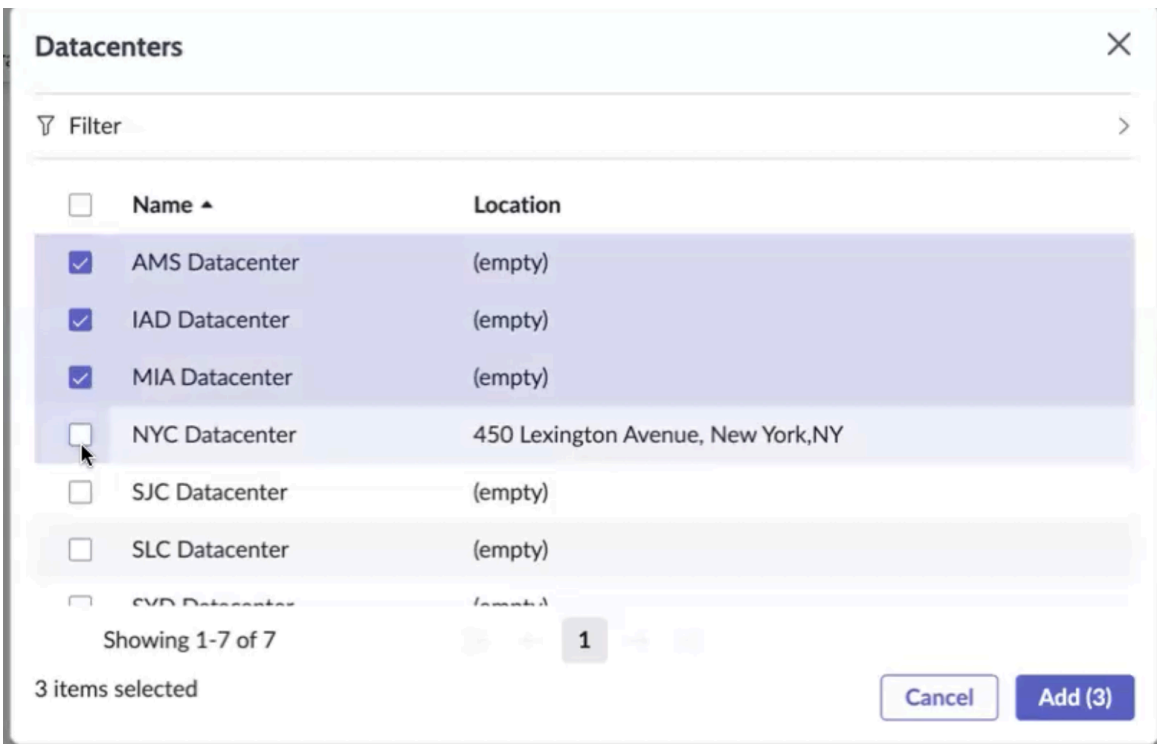



4. Navigate to **Related asset dependencies** tab and select **Add**.
   You can add the related asset dependencies to the loss of scenario as shown in the following example.




5. Select the dependencies from the list and select **Add**.

   You can add the dependencies to the loss of scenario as shown in the following example.




6. Select **Save**.
   The related asset dependencies are listed on the **Related asset dependencies** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Add a recovery strategy for the related asset dependencies

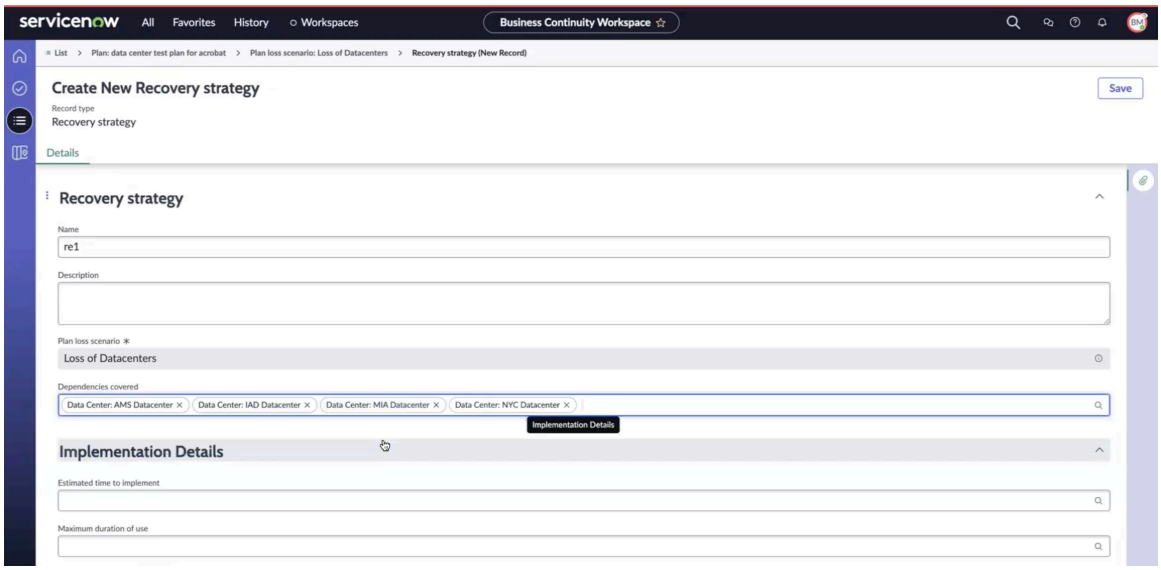
Add a recovery strategy for the related asset dependencies and estimate the time to implement the strategy. You can then get the assets up and running quickly in an identified loss scenario.

## Before you begin

Role required: sn_bcm.program_manager or sn_bcm.planner

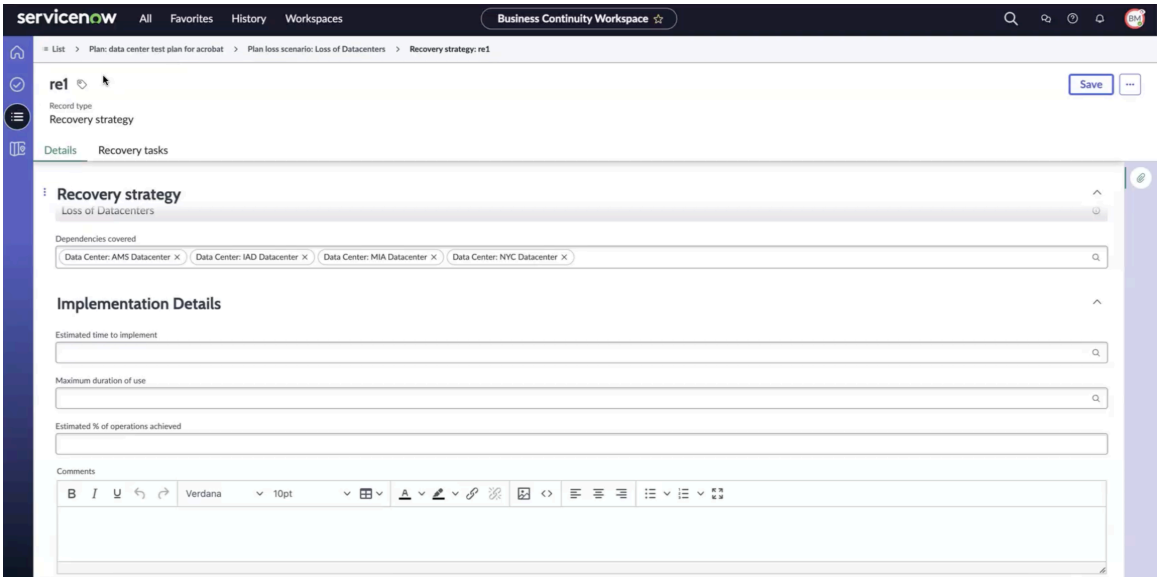
## Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to the loss scenario in the plan record.
3. Navigate to the **Recovery strategies** tab and select **New**.
   The Create new Recovery strategy form is displayed as shown in the following example.




4. On the form, fill in the fields.
   For more information on the fields in the form, see Create New Recovery strategy form.
5. Select **Save**.
   You can save the recovery strategy as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The **Recovery tasks** tab is displayed in the Recovery strategy form.

## What to do next

You can add one or more recovery tasks as part of the recovery strategy as the next step.

### Create New Recovery strategy form

Use the Create New Recovery strategy form in BCM UIB Workspace to add details about the recovery strategy for the identified loss scenario.

## Create New Recovery strategy form

For a description of the field values, see the following table.

**Create New Recovery strategy form**

| Field | Description |
|---|---|
| Details tab | |
| Name | Name of the recovery strategy for the identified loss scenario in the business continuity plan. |
| Description | Description of the recovery strategy. |
| Plan loss scenario | Loss scenario for which the recovery strategy is planned. |
| Dependencies | Dependencies that are associated with the related assets. |
| Implementation Details | |
| Estimated time to implement | Estimated time to implement the recovery strategy. |
| Maximum duration of use | Maximum duration of use for the recovery strategy. |
| Estimated % of operations achieved | Estimated % of operations achieved for the recovery strategy. |
| Comments | Comments related to the recovery strategy. The BCM administrator or planner can update the comments in the plan. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Add a recovery task for the loss scenario

Add a recovery task as part of the planned recovery strategy. You can add one or more recovery tasks for a loss scenario and those recovery tasks are displayed in the loss scenario itself. The recovery tasks that are added at the business continuity plan level are displayed on the **Recovery tasks** tab.

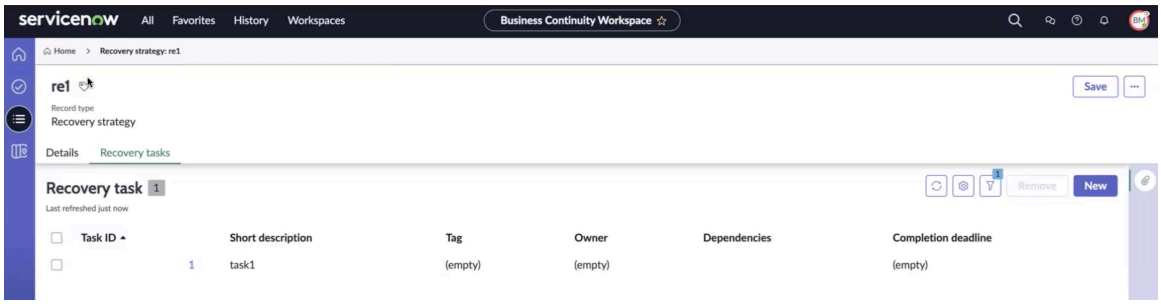
## Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

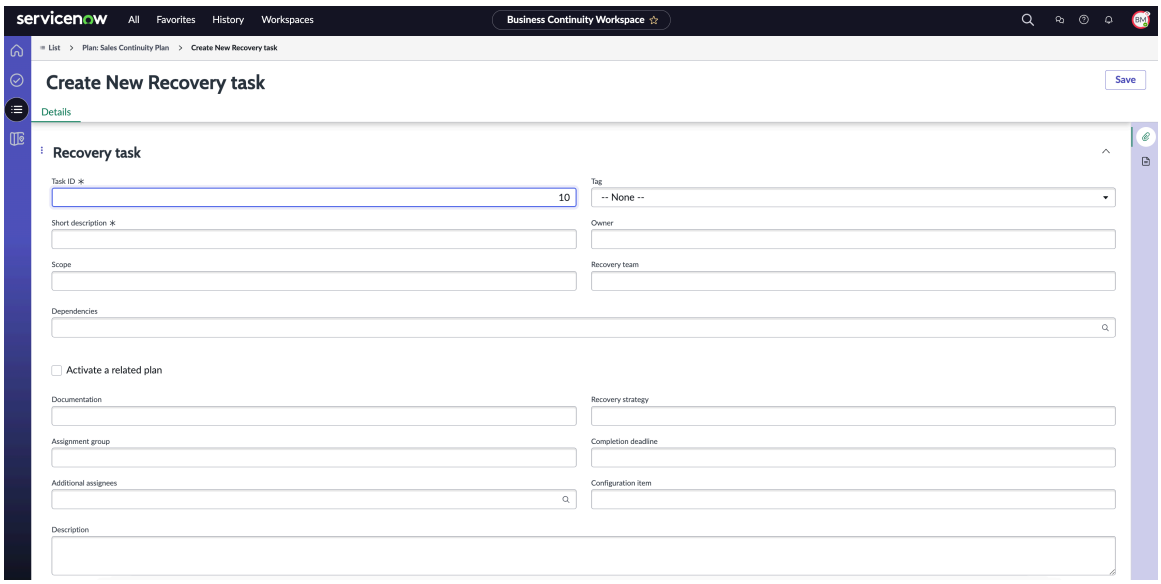
## Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to the loss scenario in the plan record.
3. Navigate to **Recovery tasks** tab and select **New**.

   You can add a recovery task to the business continuity plan as shown in the following example.



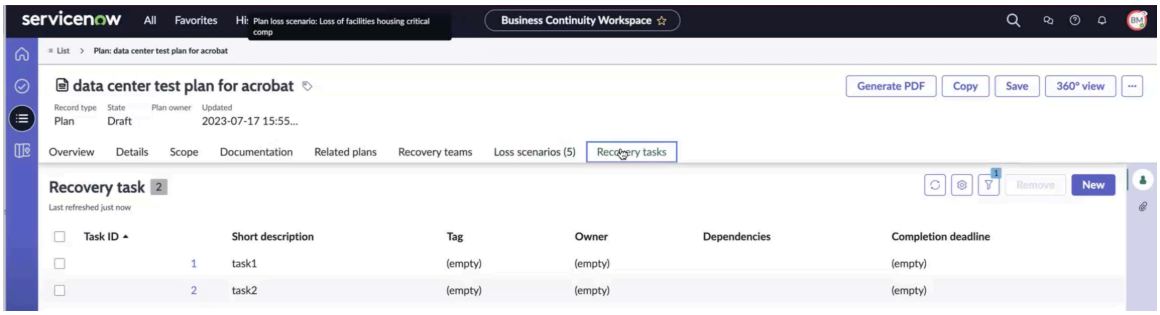

   The Create New Recovery task form is displayed.




4. On the form, fill in the fields.
   For more information on the fields in the form, see Create New Recovery task form.
5. Select **Save**.
   If the recovery task is created for one loss scenario, it is listed within that loss scenario. If the recovery tasks are created for different loss scenarios in the business continuity plan,

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the recovery tasks for all loss scenarios are listed collectively on the **Recovery tasks** tab as shown in the following example.




### Create New Recovery task form

Use the Create New Recovery task form in BCM UIB Workspace to add the details about the recovery task.

## Create New Recovery task form

For a description of the field values, see the following table.

**Create New Recovery task form**

| Field | Description |
|---|---|
| Details tab | |
| Task ID | Unique number assigned to each task. It enables you to view the tasks in a particular sequence especially in a printed PDF. |
| Short description | Short description for the recovery task. |
| Tag | Tag marked for the recovery task. |
| Owner | Assigned owner for the recovery task. |
| Scope | Asset that the task recovers. If the field is empty, the task recovers the asset at the plan level. Otherwise, it recovers the recovery task scope. |
| Dependencies | Dependencies related to the recovery task. |
| Recovery team | Team to which the recovery task is assigned. |
| Activate a related plan | Option to activate a related plan for the recovery task. |
| Documentation | Documentation section defined in the business continuity plan. |
| Assignment group | Group to which the task is assigned. |
| Recovery strategy | Recovery strategy defined on the **Recovery strategy** tab. |
| Completion deadline | Completion deadline for the recovery task. |
| Additional assignees | Additional assignees for the recovery task. |
| Configuration item | Configuration item associated with the recovery task. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create New Recovery task form (continued)

| Field | Description |
|---|---|
| Description | Description of the business continuity plan. |

## Submit the business continuity plan for an approval

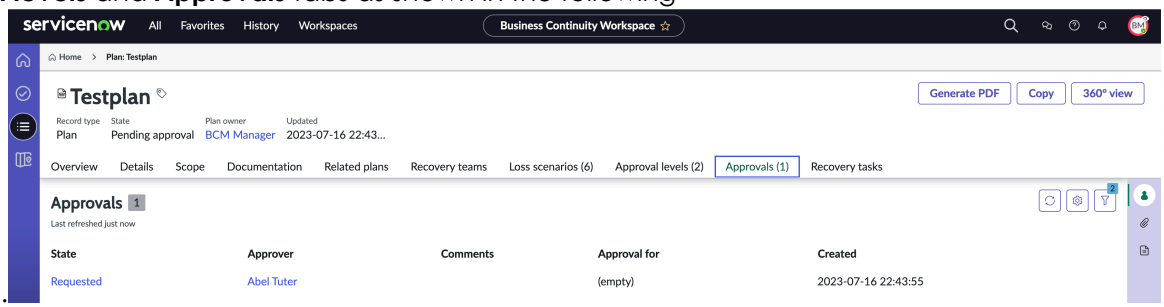
Submit the business continuity plan for an approval. You can then view the details in BCM UIB Workspace.

### Before you begin

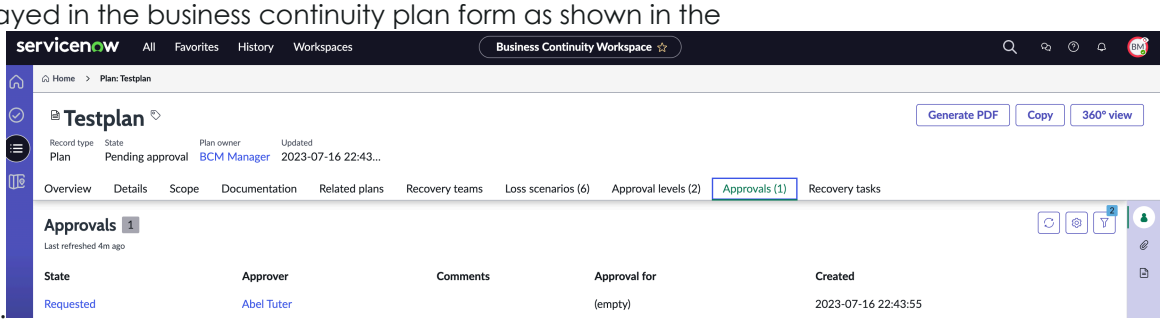
Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Planning** and select the link to the plan record in the **Name** column.
3. Select **Submit for review**.
   The business continuity plan is in the **Review** state.
4. Select **Submit for approval**.
   The business continuity plan is updated to the **Pending approval** state. The business continuity plan is submitted for a review to the business continuity plan owner.
5. Select **Approve**.
   If you have the BCM lead or BCM program manager role, you can approve the plan. The information is displayed on the **Approval levels** and **Approvals** tabs as shown in the following example.




**Note:** When you create a plan and if the approval levels and approvals requested information is listed in the **Approval levels** and **Approvals** tabs, the **Approve** and **Reject** action buttons are not displayed in the business continuity plan form as shown in the example.




When you approve the business continuity plan, its state is updated to **Approved**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Visualize the 360° relationships for a business continuity plan

Visualize the 360° relationships for a business continuity plan and its associated entities in BCM UIB Workspace. You can access the 360° view at any time while working on the business continuity plan.

### Before you begin

Role required: sn_bia.bia_admin, sn_bcm.program_manager, sn_bcm.planner

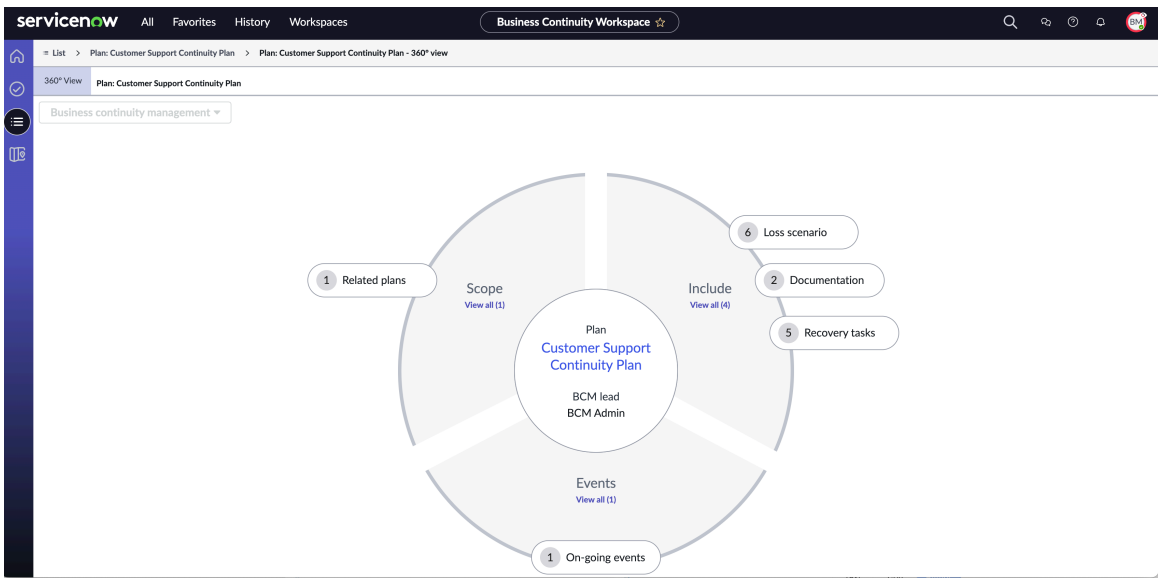
### About this task

The configurations for the 360° view are stored in **360° View Configurations** > **Configure 360° Views**. If you have the BCM administrator role, you can configure the relationships for the records in **360° View Configurations** > **Relationship Registries**.

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Planning** and select a record from the list.
   The business continuity plan record is displayed.
3. Select **360° view**.

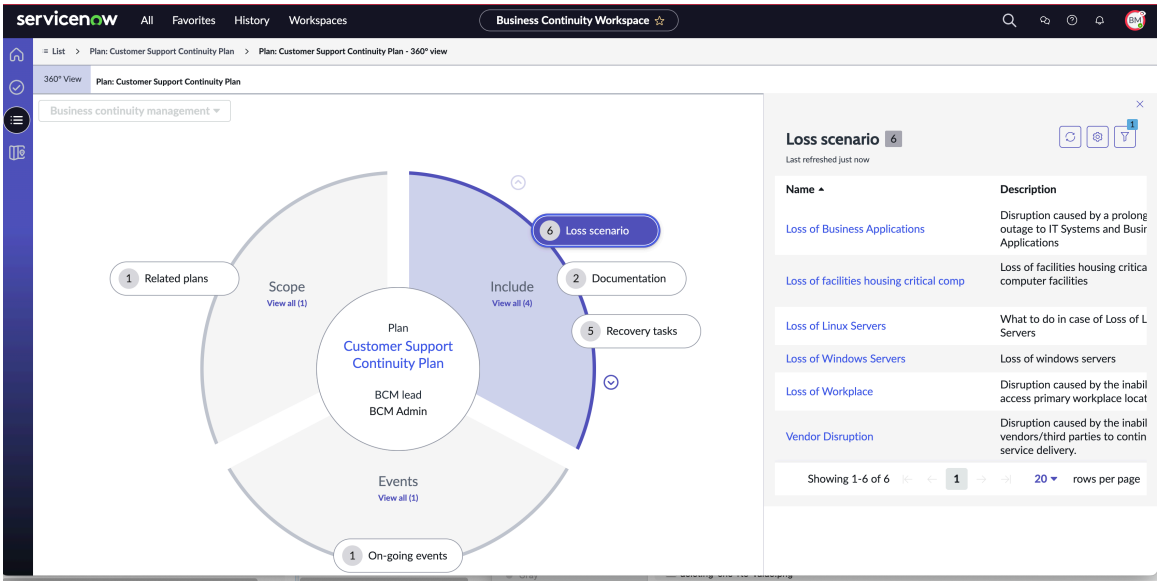
   The following example shows the 360° view of a business continuity plan and its details.




- **Name**: Name of the business continuity plan such as Customer Support Continuity Plan. You can select the business continuity plan to view its details.
- **BCM lead**: Assigned BCM lead for the business continuity plan.
- **Scope**: Scope of the business continuity plan such as **Related plans**.
- **Events**: Events that are associated with the business continuity plan such as **Ongoing events**.
- **Include**: Entities that are associated with the business continuity plan such as **Loss scenario**, **Documentation**, and **Recovery tasks** as shown in the following example.

The following example shows the 360° relationship view for the Customer Support Continuity Plan and its related entities. When you select the **Loss scenario** capsule in the 360° view, the details of the associated loss scenarios for the Customer Support Continuity Plan are displayed in the Loss scenario panel on the right.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




4. To navigate to the plan again, select the plan or list view in the breadcrumb navigation.

## Generate the PDF of a business continuity plan

Generate a PDF of a business continuity plan in BCM UIB Workspace and save it for a future reference.

### Before you begin

Role required: sn_bcm.program_manager, sn_bcm.planner

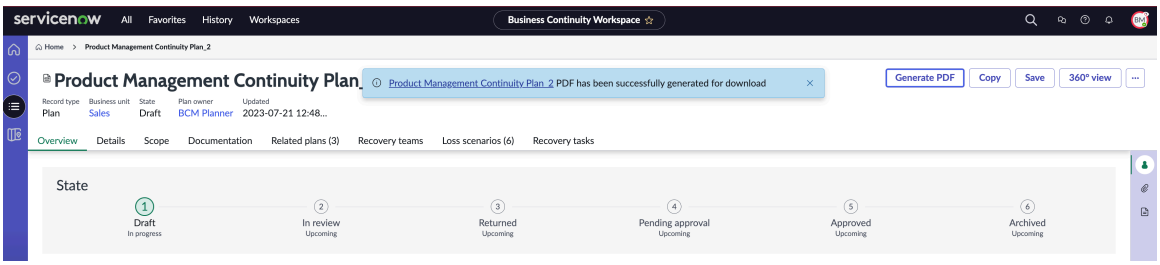
### About this task

To format the PDF for your business needs, see Format the PDF templates for BIA, BCP, and Events.

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Planning** and select any business continuity plan record that is in the **Review** or next state.
3. Select **Generate PDF** in the form.

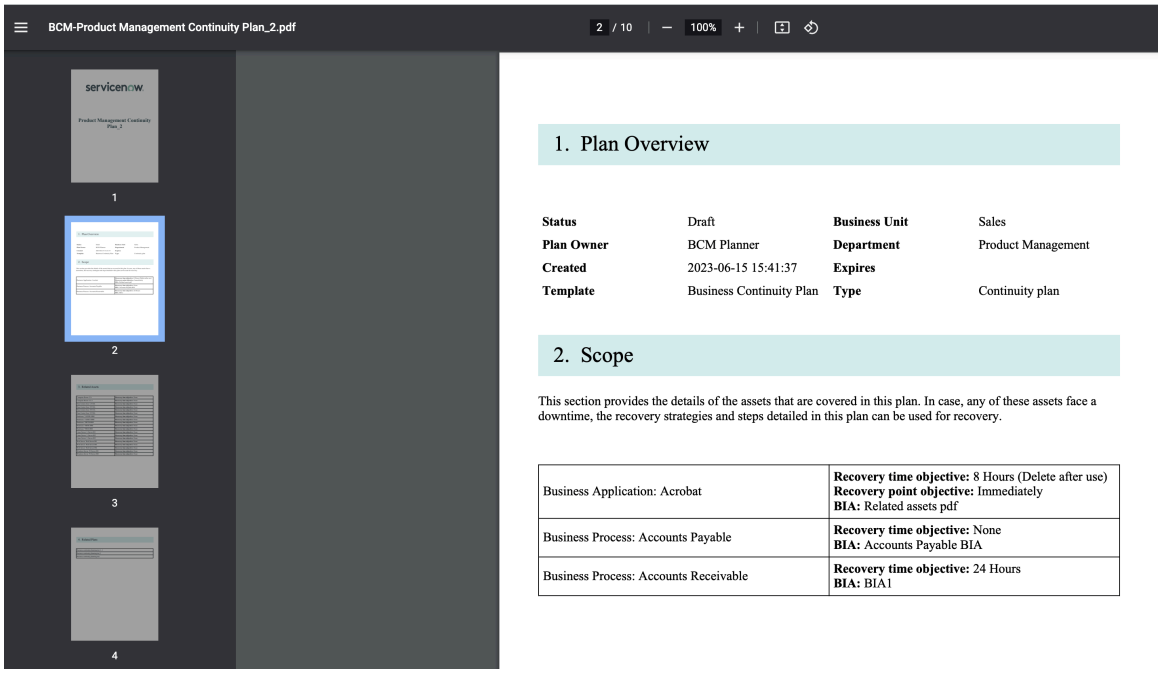
   The following example shows the message that is displayed on the screen: `<Name of the BCP> PDF has been successfully generated for download.`




4. To download the PDF, select the link in the message and open the PDF.

   The following example shows the PDF of a business continuity plan.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




5. Save the PDF on your system.
   You can save the PDF for a future reference.

## Structured workflows for Exercise Management in BCM UIB Workspace

Perform the structured workflows that are outlined in this section to manage an exercise in Business Continuity Workspace (also known as BCM UIB Workspace).

Typically, the BCM program manager performs the following tasks to exercise an event:

- Create an exercise. For more information, see Create an exercise.
- Add an asset and plan to the exercise. For more information, see Track the impacted assets and add a related plan.
- Add an event task to the exercise. For more information, see Add a task to the exercise.
- Submit the event task for the exercise event. For more information, see Approve the exercise.

## Additional information on Exercises

- For information on the **Exercises** tab in the Home page, see Home page view.
- For information on the exercises, see Exercises.

### States for an exercise and crisis event

This section describes the states of progression for an exercises and crisis event.

## States for an exercise and crisis event

### States for an exercise and crisis event

| State | Description |
|---|---|
| **Pending** | First state of the event. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States for an exercise and crisis event (continued)**

| State | Description |
|---|---|
| **Pending Approval** | State of the event when an approval is requested. When you select **Submit for Approval**, the event is set to the **Pending Approval** state. In this state, you can only update the **Work notes** field in the event form.<br><br>If any approval rules are configured for the event, then the approvals are generated and sent to the approvers. If no approval records are associated with the event in the requested state, then you can either select **Reject** or **Approve**.<br><br>You can view the approval details of an event in the**Approvals** tab with the name of the approver, level of approval, and state of the approval.<br><br>You can view the approval history of the event in the **Approval History** tab such as the approval state, name of the approver, event number, and so on.<br><br>**Note:** If you are a BCM program manager, you can see the **Approve** and **Reject** buttons. |
| **Returned** | State of the event when an event is rejected. The state is set to **Returned**. It can be moved to the **Submit for Approval**, **Closed Complete**, or **Closed Incomplete** states. Since this action is related to an event only, you can update the description, results, and work notes in the form.<br><br>When an event is in the **Returned** state, you can edit the state of the event asset.<br><br>From the **Returned** state onwards, you can only add your comments and the attachments to the event task. |
| **Closed Complete and Closed Incomplete** | States of the event when an event is approved. You can close the approved event. You can set the event state to either **Closed Complete** or **Closed Incomplete** by selecting **Close Event**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States for an exercise and crisis event (continued)**

| State | Description |
|---|---|
| **Approved** | Final state of the event. When an event is approved, the state is set to the **Approved** state.<br><br>You can perform the following additional UI actions:<br><br>Generate PDF<br><br>Download the PDF of an exercise or crisis event for reference. When you select Generate PDF, the PDF attachment is available in the **Activity** panel of the **Details** tab.<br><br>For information on generating the PDF of an exercise or crisis event, see Generate the PDF of an exercise or crisis event.<br><br>Copy<br><br>Save a copy of an exercise or crisis event for future reference as a template.<br><br>360° view<br><br>Visualize the 360° representation of an exercise or crisis event.<br><br>For information on how to view 360° relationships of an exercise or crisis event, see Visualize the 360° relationships for an exercise and crisis event.<br><br>Delete<br><br>Delete an exercise or crisis event.<br><br>Edit<br><br>Edit an exercise or crisis event.<br><br>Save<br><br>Save an exercise or crisis event. |

See the following state transitions of an event task.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### State transitions of an event task

| State | Description |
|---|---|
| **Open** | Open state of the event task. When an event is started, its event tasks that do not have a dependent recovery task move to the **Open** state. |
| **Pending** | Pending state of the event task. The event tasks that are dependent on other recovery tasks are in the **Pending** state when the event is started. After the dependent tasks are closed, the parent event task moves to the **Open** state. |
| **Skip Task** | Skip Task action for the event task. This action is available only if you have logged in as the BCM program manager. The **Skip**action is displayed when the task is in the **Pending** or **Open** state and the event must be in **Work in Progress** state. Selecting **Skip Task** moves the task to the **Closed Skipped** state. The actual start time and actual end time at this state are empty. |
| **Trigger** | Trigger action for the event task. This action is available only if you have logged in as the BCM program manager. The task is in the **Pending** state. Selecting **Trigger** moves the task to the **Open** state irrespective of its dependencies. |
| **Work In Progress** | Work In Progress state of the event task. The task is in the **Open** state. Selecting **Work In Progress** moves the task to the **Work in Progress** state. You can update the actual start time of the task in the **Actual start** field in this state. If you do not update the actual start time, the current date and time are recorded as the actual start time. The next available options are **Closed Complete** or **Closed Incomplete** state. |
| **Closed Incomplete** | Closed Incomplete state of the event task. Actual end time of the task is recorded in the **Actual end** field. If you do not update the actual end time, the current date and time are recorded as the actual end time. Update necessary information in the **Work notes** field and save the task. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### State transitions of an event task (continued)

| State | Description |
|---|---|
| **Closed Complete** | Closed Complete state of the event task. The task is closed and complete in this state. Actual end time of the task is recorded in the **Actual end** field. If you do not update the actual end time, the current date and time are recorded as the actual end time. |

## Create an exercise

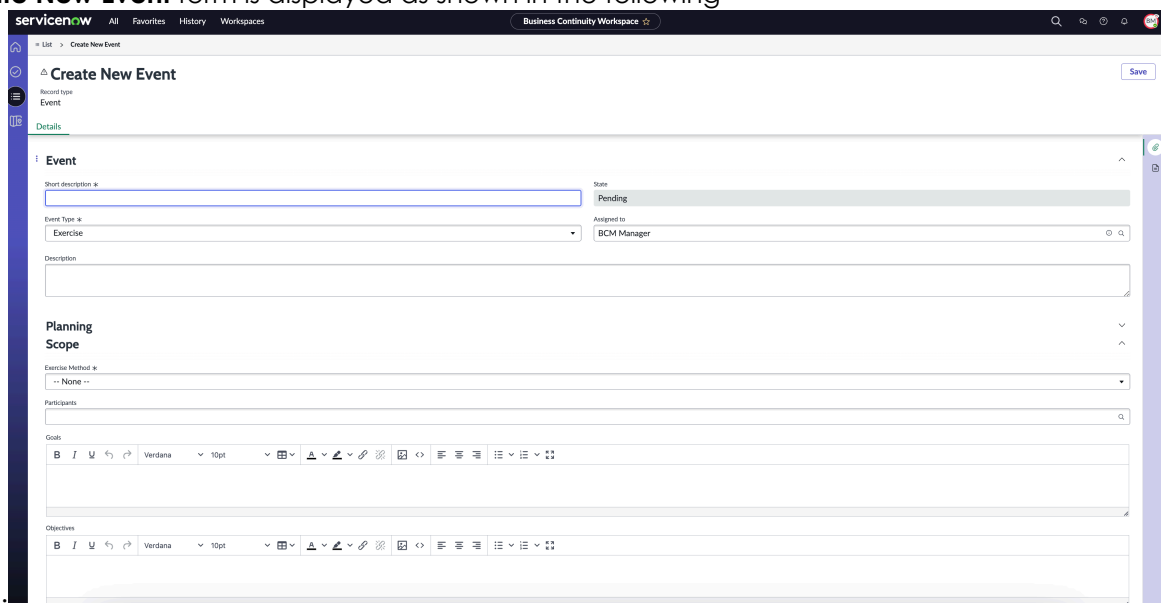
Create an exercise in BCM UIB Workspace. You can then test your business continuity and recovery plans on a planned date and monitor the completion of the event tasks.

### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Exercises** > **Pending** and select **New**.
   The **Create New Event** form is displayed as shown in the following example.

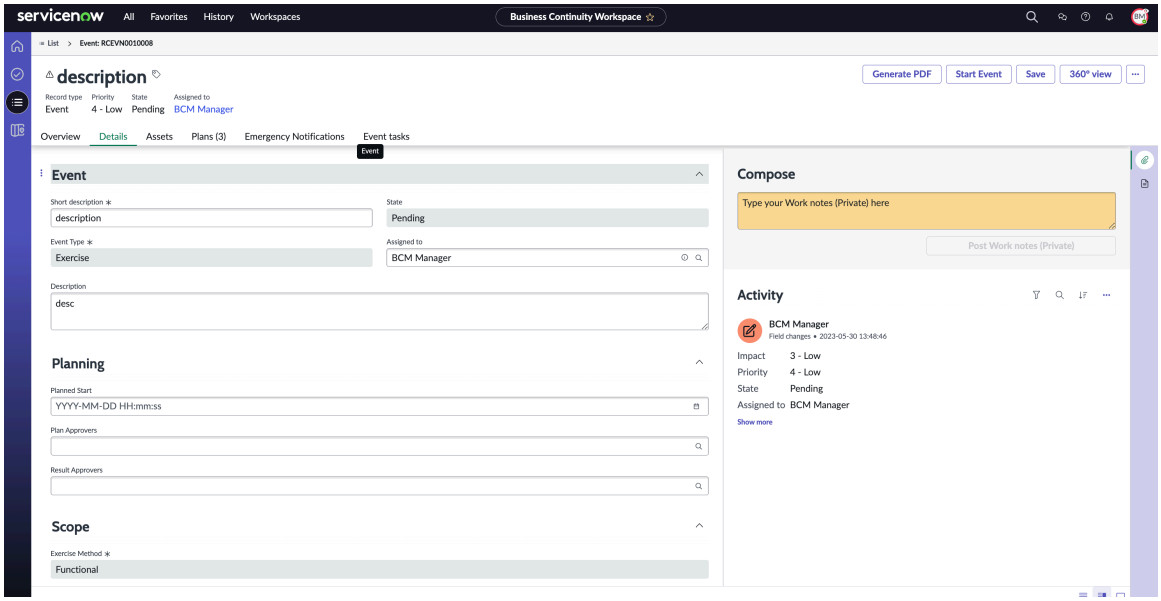



3. In the **Details** tab of the **Create New Event** form, fill in the required fields.
   For more information on the fields, see Create Exercise Event form.
   The exercise event is created in the **Pending** state and it is displayed in the List view. The state and details of the exercise event are displayed in the following tabs:
   - **Overview**: You can view the current state and overall state progression of the exercise event.
   - **Details**: You can update the fields in the form such as **Short description**, **Assigned to**, **Exercise method**.
   - **Assets**: You can select the impacted item type or the primary elements that you want to recover for an asset type.
   - **Plans**: You can add an ad-hoc plan for the selected asset to the event.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Emergency Notifications**: You can create an emergency notification for the exercise event.
- **Event tasks**: You can add an ad-hoc task to the event.

The Exercise event form is shown in the following example.




4. Select **Save**.
   The exercise event is saved in the **Pending** state.

### Create Exercise Event form

Use the Create Exercise Event form in BCM UIB Workspace to add details about an Exercise event.

## Create Exercise Event form

For a description of the field values, see the following table.

### Create Exercise Event form

| Field | Description |
|---|---|
| Details tab | |
| Short description | Brief description about the event. |
| Event type | Type of the event. For exercise events, the event type is **Exercise**. |
| State | Defaults to the **Pending** state. |
| Assigned to | User or users from the Assignment group. If the **Assignment group** field is empty, then select any user. |
| Description | Description of the exercise event. |
| Planning | |
| Planned Start | Planned start date for the exercise event in the *YYYY-MM-DD HH:mm:ss* format. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create Exercise Event form (continued)**

| Field | Description |
|---|---|
| Plan Approvers | Plan approvers for the exercise event. |
| Result Approvers | Result approvers for the exercise event. |
| Scope | |
| Exercise Method | Method for the exercise. Available options are:<br>• **Simulation**<br>• **Tabletop**<br>• **Walkthrough**<br>• **Functional**<br>**Note:** For exercise events, the exercise method is **Functional** by default. |
| Participants | Participants for the exercise. |
| Goals | Goals for the exercise. |
| Objectives | Objectives for the exercise. |

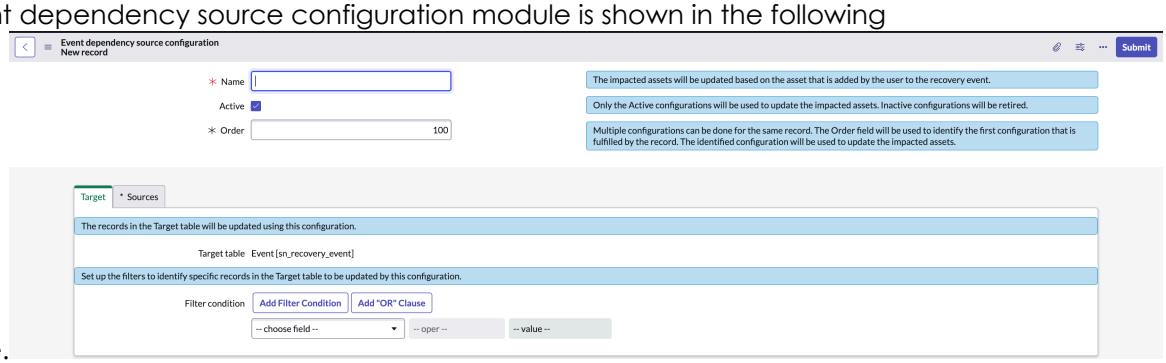
### Add the dependencies of the impacted assets manually in the events

You can add the dependencies of the impacted assets in the events and exercises based on the source data and relationships in the CMDB, BIAs, and plans.

## Configuring the sources in the Event dependency source configuration module

The BCM administrators can configure the sources to get the event dependencies in the Event dependency source configuration module.

The Event dependency source configuration module is shown in the following example.




When the BCM administrators can update the target records, filter condition for the records, and sources to fetch the event dependency.

Dependencies are added in the events only when the user selects the **Update dependencies** UI action. Dependencies are fetched from the following sources for the events:

- BIA upstream dependency
- BIA downstream dependencies

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- CMDB
- Plan primary assets
- Plan related assets

**Note:** In an event, the dependencies of all assets are added manually where the source is Manual.

Setting up the Event dependency source configuration module is a one-time activity. Once the sources are configured in the Event dependency source configuration module, the updates are synchronized in the events.

For more information on setting up the Event dependency source configuration module, see Configure the Event dependency source configuration module.

## Roles associated with event dependency updates

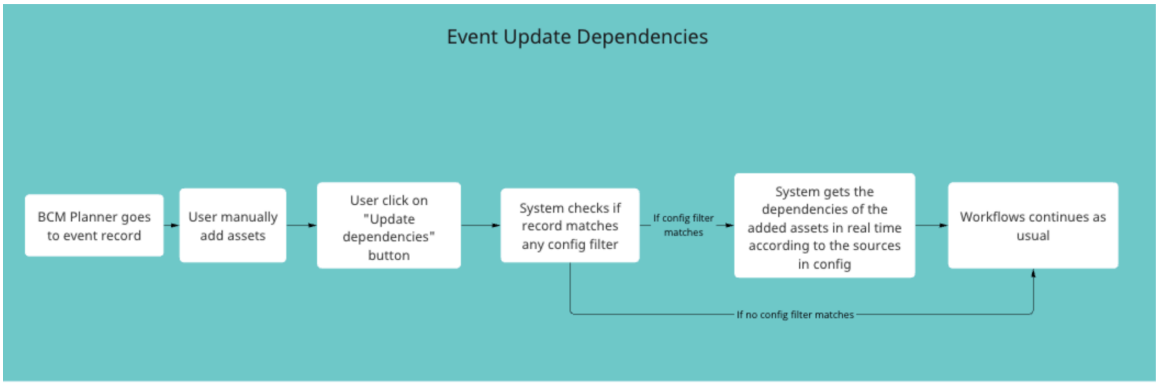
Users with the following roles typically check for the dependency updates in an event:

- The BCM program managers, BCM planners, and BCM managers can update the latest dependencies.
- BCM administrators can configure the Event dependency source configuration module.

## Workflow for updating the dependencies manually in the events and exercises

As the BCM application user, when you select the **Update dependencies** UI action in the Event record, the dependencies of all assets are added manually where the source is Manual.

The BCM application executes a workflow to update the impacted assets in the events and exercises as shown in the following example.




1. The BCM planner navigates to the event record.
2. The BCM planner selects the **Update dependencies** UI action to add the assets manually.
3. The application checks if the event record matches any configuration filter.
4. If the event record matches any configuration filter, the system gets the dependencies of the added assets in real time according to the sources defined in the configuration (Event dependency source configuration module).
5. If the event record does not match any configuration filter, the events workflow then continues for the next steps, the events workflow then continues for the next steps.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information on updating the event dependencies manually, see Update the event dependencies manually.

## Data Relationships Framework

Beginning with the Utah release, the Data Relationships Framework application (com.sn_app_grc_relationship_config) supports the BCM application with the underlying framework to add the dependencies of the impacted assets in the events and exercises. The Data Relationships Framework application is installed with the BCM application by default.

For more information on the Data Relationships Framework, see Data Relationships Framework.

### Update the event dependencies manually

Update the event dependencies manually by selecting the **Update dependencies** UI action. You can update the dependencies in an active event.

#### Before you begin

Role required: sn_bcm.program_manager, sn_bcm.planner, sn_bcm.admin

#### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. Open an event in the **Pending** state.
3. To update the dependencies manually, select **Update dependencies**.
   A UI message is displayed on the screen: `Dependencies are being updated.`
4. To save the changes to the event, select **Save**.
   The plan owners and BCM lead can update the event dependencies by saving the changes to the event.

### Track the impacted assets and add a related plan

Track the impacted assets and add a related plan to the exercise. You can then monitor the assets and plans for the exercise in BCM UIB Workspace.

#### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

#### Procedure

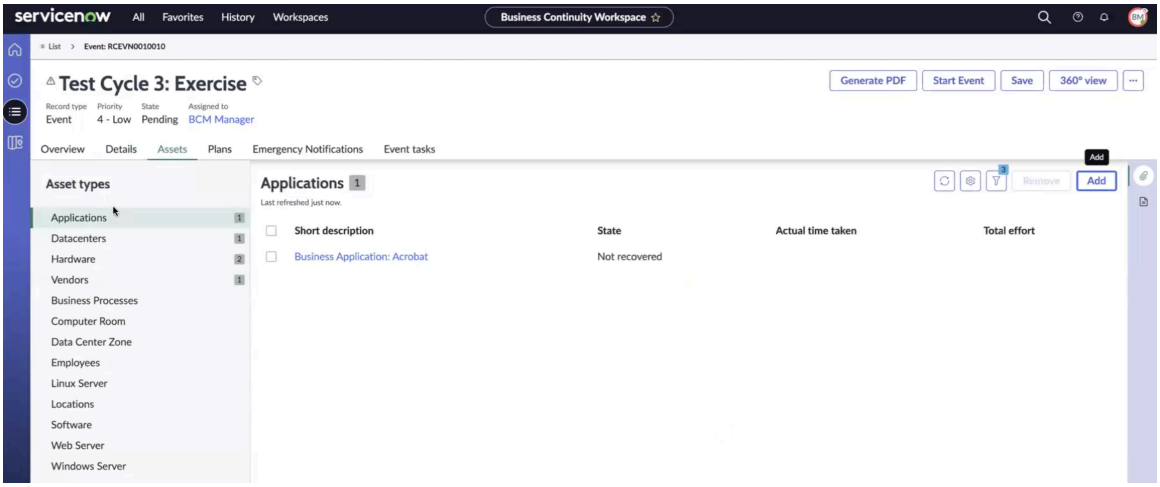
1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Exercises** > **Pending** and select the exercise event in the list.
3. In the **Assets** tab, select **Add**.

   You can add an asset that you want to recover during the exercise. The primary elements of the asset are listed as **Asset types**. The primary elements belong to the element definition type that is identified in the plan template. When you add an asset to the event, its associated dependencies are pulled into the event. The dependencies are displayed in the **Asset types** panel.

   **Note:** When you select **Add** for an application, all the dependencies that you had identified in the business impact analysis of that application are also added to the exercise.

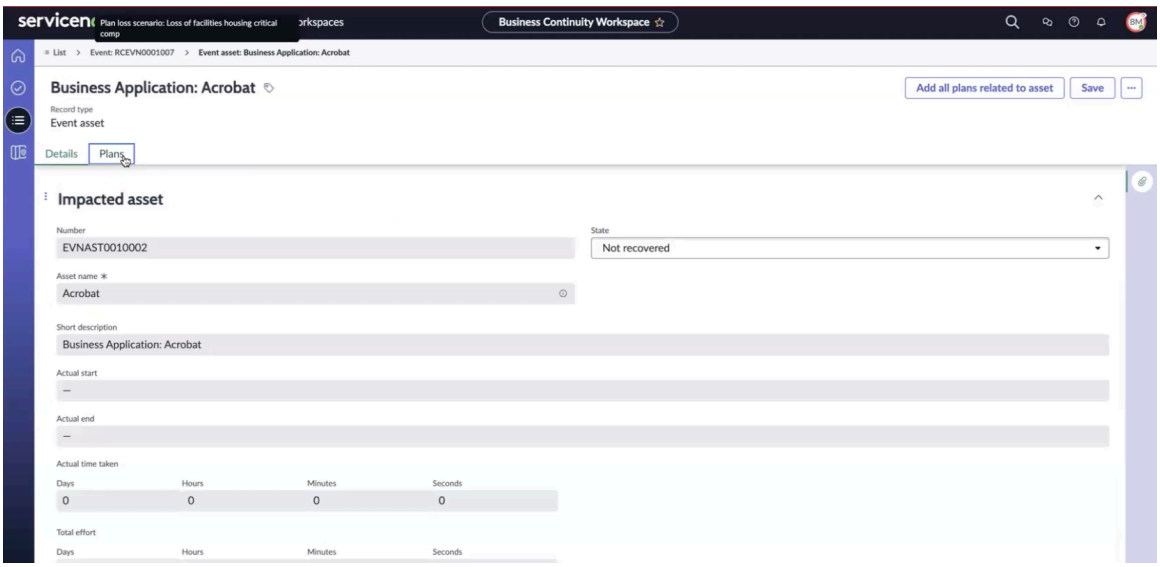
   The following example shows the dependencies for Business Application: Acrobat in the **Asset types** panel of the exercise.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



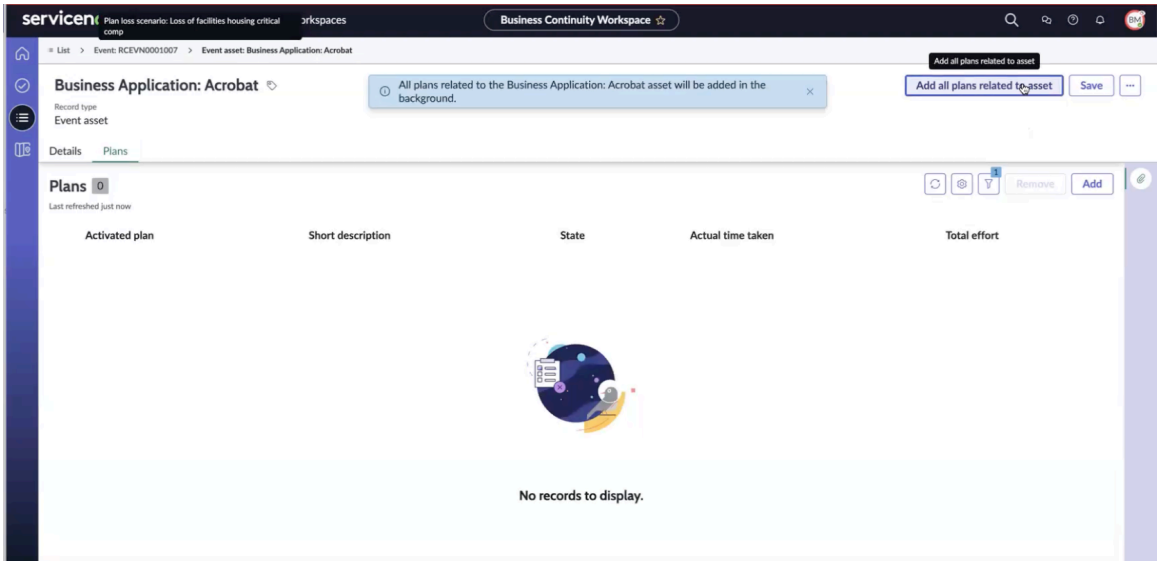

**4.** In the Applications list, select the application and navigate to the **Plans** tab.

You can navigate to the **Plans** tab as shown in the following example.




**5.** Select **Add all plans related to asset**.
All plans that are related to the selected application are added to the exercise.
An informational message is displayed that all plans related to the selected application are added in the background as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




6. Select **Save**.
   The exercise is saved in the **Pending** state.

### Add a task to the exercise

Add a task to the exercise in BCM UIB Workspace. You can then monitor and complete the tasks that are associated with the exercise.

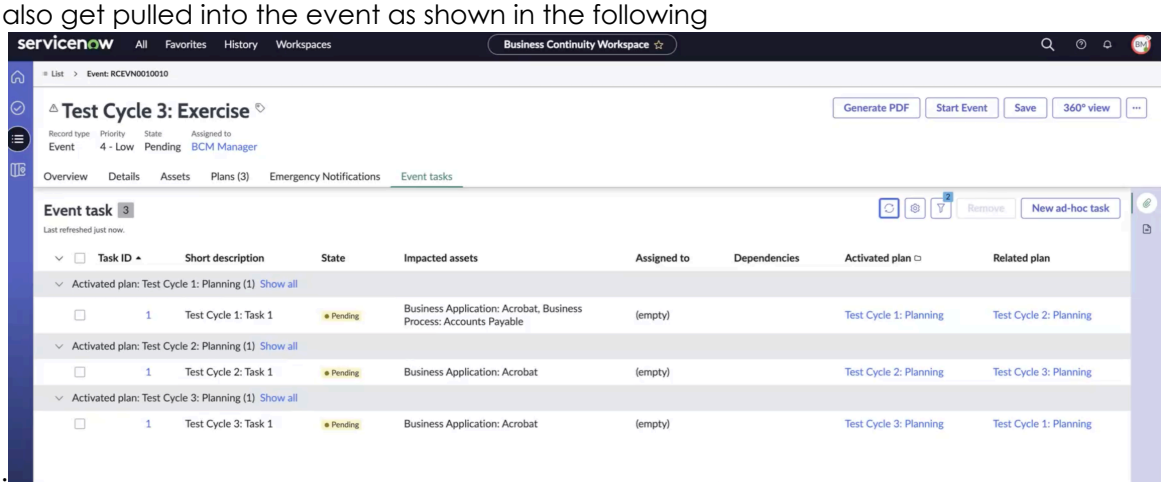
**Before you begin**
Role required: sn_bcm.planner, sn_bcm.program_manager

**Procedure**

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Exercises** > **Pending** and select the exercise event in the list.
3. Select the **Event tasks** tab.

> **Note:** The **Event tasks** tab is displayed for the exercise events when the exercise method is **Functional**.

When you add or update the plan to the exercise event, the related plans, assets, and event tasks that are associated with the plan also get pulled into the event as shown in the following example.




The following example shows the circular tasks where Task 3 has a dependency on Task 1.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Test Cycle 1: Task 1 activates Test Cycle 2: Planning.
- Test Cycle 2: Task 1 activates Test Cycle 3: Planning.
- Test Cycle 3: Task 1 activates Test Cycle 1: Planning.

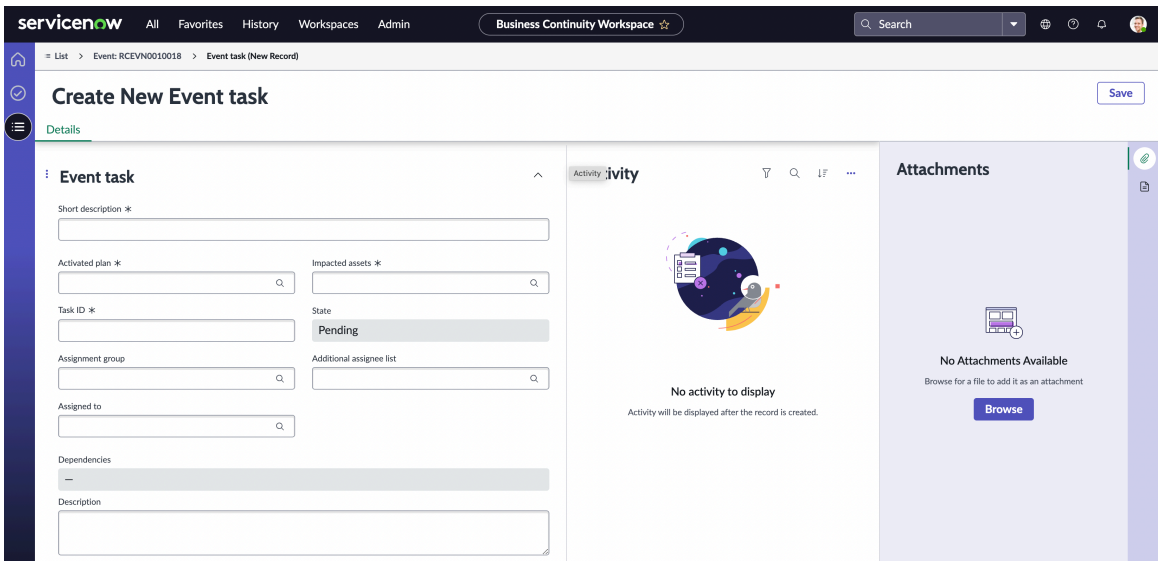
4. To add an ad-hoc task to the event, select **New ad-hoc task**.

> **Note:** When you add an ad-hoc task to the exercise event that is in the **Work in progress** state and if the activated plan is in the **Work in progress** state, the tasks will be in the **Open** state. If the activated plan is the **Pending** state, the task will be in the **Pending** state.

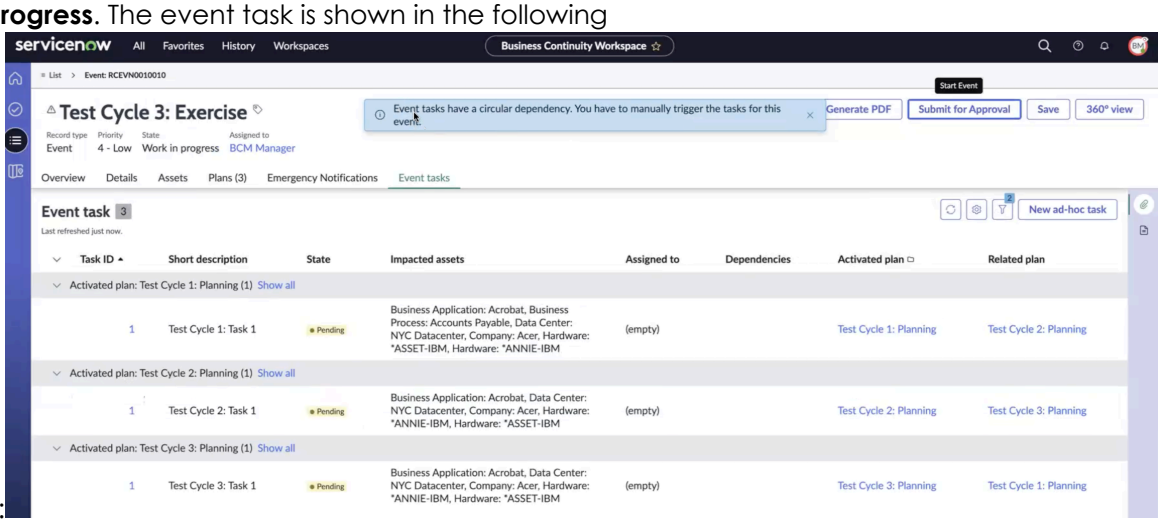
For more information on the fields in the New Event Task form, see Create New Event Task form.

> **Note:** You cannot create an ad-hoc task for the activated plans that are in **Closed Complete** or **Closed Incomplete** state.

The **Create New Event task** form is displayed as shown in the following example.




5. To start the exercise, select **Start Event**.
After you start the exercise, the event state is updated to **Work in Progress**. The event task is shown in the following example:

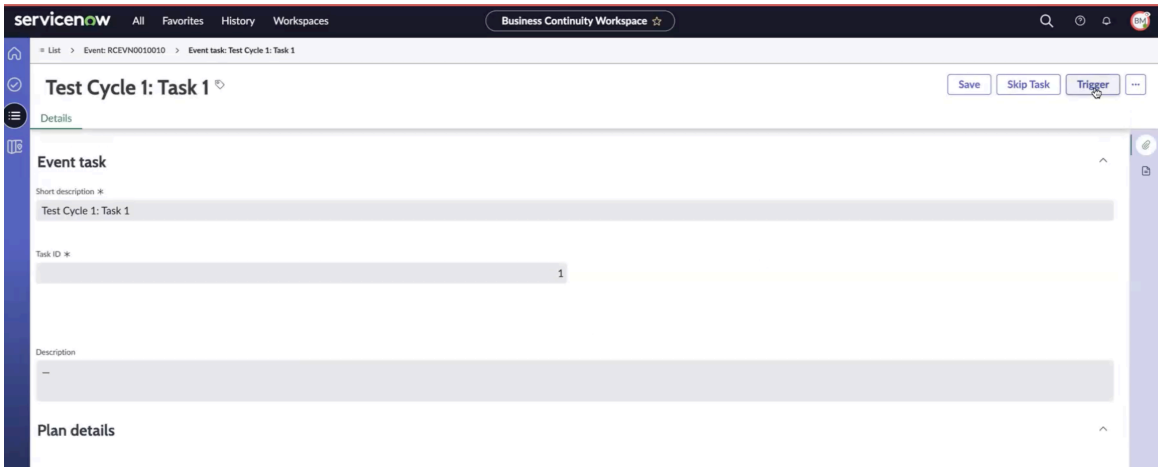



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

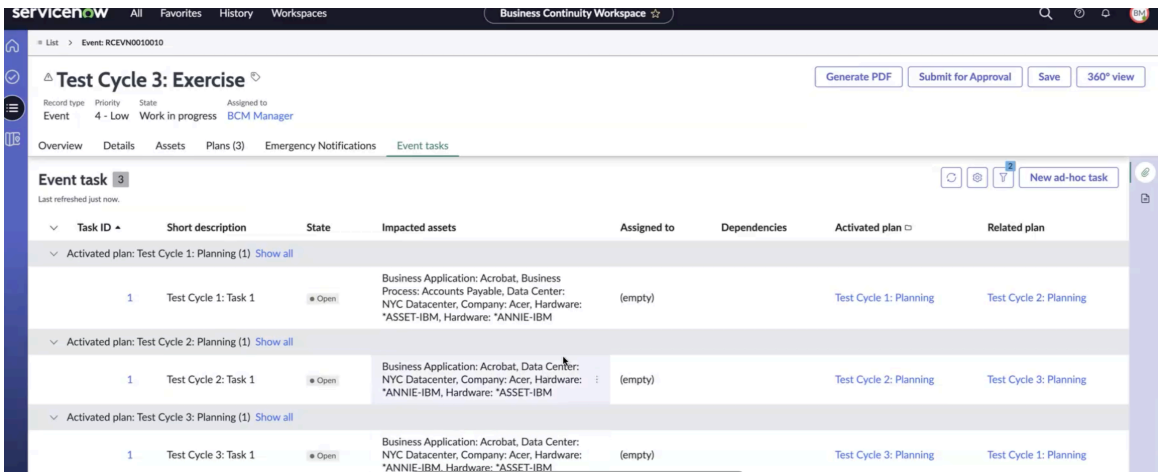
A message is displayed that the event task has a circular dependency. You have to trigger the tasks manually for this event.

6. Select the first task and select **Trigger**.

   The process to trigger the task manually is shown in the following example.




   It updates the state of the task to **Open** as shown in the following example and opens all the dependent tasks one by one.




7. Complete all the activated plans of the event tasks for the exercise event and select **Submit for Approval**.
8. To generate a PDF, select **Generate PDF**.
   If you have edit access to the crisis event, you can save a copy of the event in PDF format to your local hard drive.

   **Note:** By default, the PDF is generated and attached after the event is closed.

9. Navigate to the **Results** section on the **Details** tab and update the **Actual start** and **Actual end** dates for the event task.
10. Update the assignment fields, if necessary.
11. Enter any event task-related information in the **Work notes** field of the **Activity** section.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

12. Select **Save**.

13. Select the refresh icon ( ) to display the updated state of the asset or plan, and the actual time taken to recover the asset.

### Create New Event Task form

Use the Create New Event Task form in BCM UIB Workspace to add details about an event task.

## Create New Event Task form

For a description of the field values, see the following table.

**Create New Event Task form**

| Field | Description |
|---|---|
| Details tab | |
| Short description | Brief note about the event task. |
| Activated plan | Activated plan for the event task. |
| Impacted assets | Assets that are impacted for the event task. |
| Task ID | Defaults to the next number of existing event tasks for the plan. |
| State | Defaults to **Pending** state. |
| Assignment group | Group to which the event task is assigned. |
| Additional assignee list | Additional users that are assigned to the event task. |
| Assigned to | User or users from the Assignment group. If the **Assignment group** field is empty, then select any user. |
| Dependencies | Dependencies for the tasks. For tasks copied from the plan level, dependencies are copied from the plan recovery task. Dependencies cannot be added for ad-hoc tasks. |
| Description | Information about the event task. |
| Activity | |
| Work notes | Information about the event task shared internally. |

### Approve the exercise

Approve the exercise in BCM UIB Workspace.

## Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager

## Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Exercises** > **Pending** and select the exercise event in the list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Log in as the approver of the event and select the Event in the List view.
4. Select **Closed Incomplete**.
   If the event tasks associated with the event are not complete, you can update the state of the event to **Closed Incomplete**.
5. Select **Submit for approval**.
6. Select **Closed Complete**.
   You can update the state of the event to **Closed Complete**.

### View your recovery tasks from Self-Service

View the recovery tasks that are assigned to you or the recovery task team to recover assets from a crisis event or exercise. Your BCM program manager assigns the tasks to you and you can view them from the self-service application menu.

#### Before you begin
Role required: sn_bcm.recovery_team_member

#### Procedure
1. Navigate to **Self-Service** > **My Recovery Tasks**.
2. View the list of the event tasks that are assigned to you, the assigned group that you are part of, or a recovery team that you belong to and the state of the event is not in the **Pending** state.
   You can view the name and description of the recovery task.
3. Select the link to the **Task ID** of an event task that you want to update.
   You can update the **Actual start** and **Actual end** details.
4. Sort the **Event Type** column to list the crisis-related tasks at the top.
5. View the **Event Task type** column to understand whether it is planned or an ad-hoc event.
6. To add any notes to the event task activity, select the **Activity** section on the **Details** tab and add the information in the **Work notes** field.
7. To update the task to an **In progress** state, select **Work in Progress**.
8. To close the task, select either **Close Incomplete** or **Close Complete**.
9. To update the record, select **Update**.

### Visualize the 360° relationships for an exercise and crisis event

Visualize the 360° relationships for an exercise or a crisis event and the associated entities in BCM UIB Workspace. You can access the 360° view at any time while creating an exercise and a crisis event.

#### Before you begin
Role required: sn_bia.bia_admin, sn_bcm.program_manager, sn_bcm.planner

#### About this task
The configurations for the 360° view are stored in **360° View Configurations** > **Configure 360° Views**. If you have the BCM administrator role, you can configure the relationships for the records in **360° View Configurations** > **Relationship Registries**.

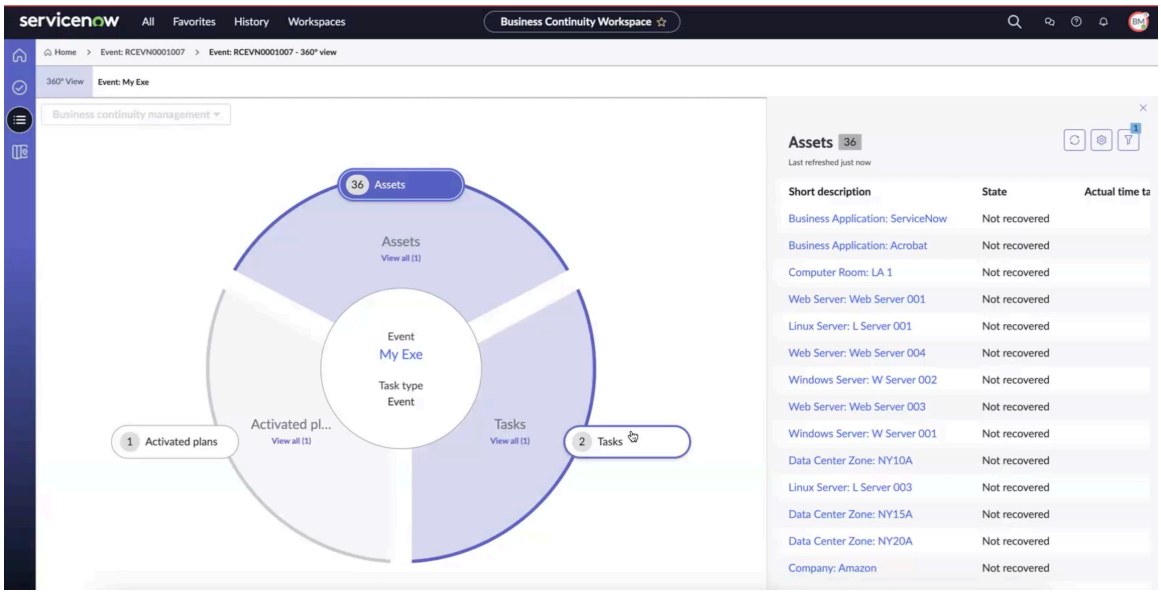
#### Procedure
1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Exercise** and select a record from the list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The exercise event record is displayed. The same procedure applies for a crisis event.

3. Select **360° view** in the event record.

   The 360° view for the selected event is displayed as shown in the following example.




   The 360° view for the selected event shows the following details:

   - **Activated plans**: Activated plans that are associated with the assets.
   - **Assets**: Assets that are impacted due to the event.
   - **Tasks**: Tasks that are associated with the event.

   When you select the **Assets** capsule in the 360° view, the details of the assets for the event are displayed in the **Assets** panel on the right as shown in the example.

4. To navigate to the event again, select the event or list view in the breadcrumb navigation.

### Generate the PDF of an exercise or crisis event

Generate the PDF of an exercise or a crisis event in BCM UIB Workspace and save it for a future reference.

#### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager

#### About this task

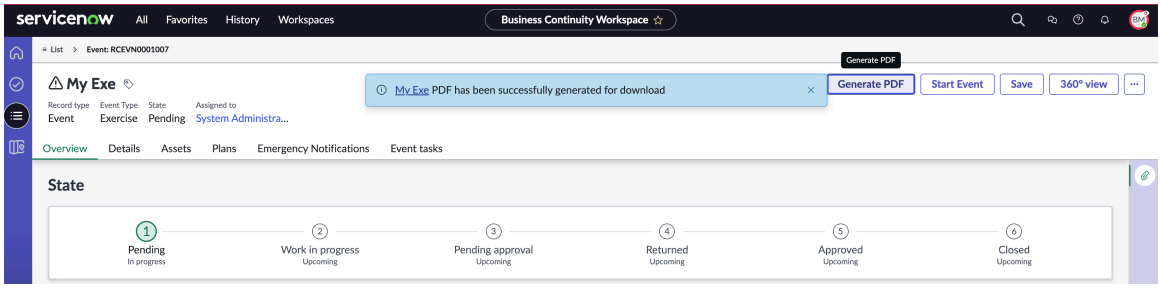
To format the PDF for your business needs, see Format the PDF templates for BIA, BCP, and Events.

#### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Exercises** and select any event record that is in the **Review** or next state.
   You can use the same process of generating the PDF for a crisis event.
3. Select **Generate PDF** in the form.

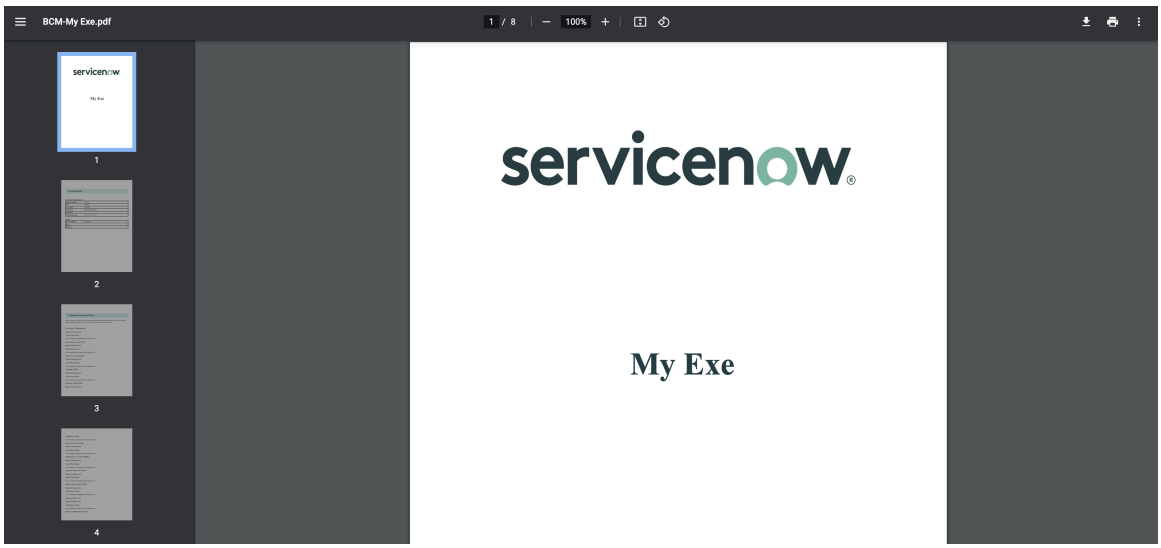
   The following example shows the message that is displayed on the screen: `<Name of the exercise event> PDF has been successfully generated for download.`

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




4. To download the PDF, select the link in the message.

   The following example shows that the PDF of the exercise has been downloaded locally.




5. Save the PDF on your system.
   You can save the PDF for a future reference.

## Structured workflows for Crisis Management in BCM UIB Workspace

Perform the structured workflows to manage a crisis event in Business Continuity Workspace (also known as BCM UIB Workspace).

Typically, the BCM program manager performs the following tasks to respond to a crisis event:

- Create a crisis event. For more information, see Start a crisis event.
- Add an asset and plan to the crisis event. For more information, see Track the impacted assets and add a related plan.
- Add an event task to the crisis event. For more information, see Add a task to the crisis event.
- Submit the event task for the exercise event. For more information, see Approve the crisis event.

## Additional information on Crisis events

- For information on the **Crisis events** tab in the Home page, see Home page view.
- For information on the threats, feeds, and alerts in the Crisis map interface, see Crisis map interface.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- For information on the administrative tasks in the Crisis map interface, see Setup for Crisis map.
- For information on the crisis events, see Crisis events.

### Start a crisis event

Start a crisis event in BCM UIB Workspace.

**Before you begin**
Role required: sn_bcm.planner, sn_bcm.program_manager

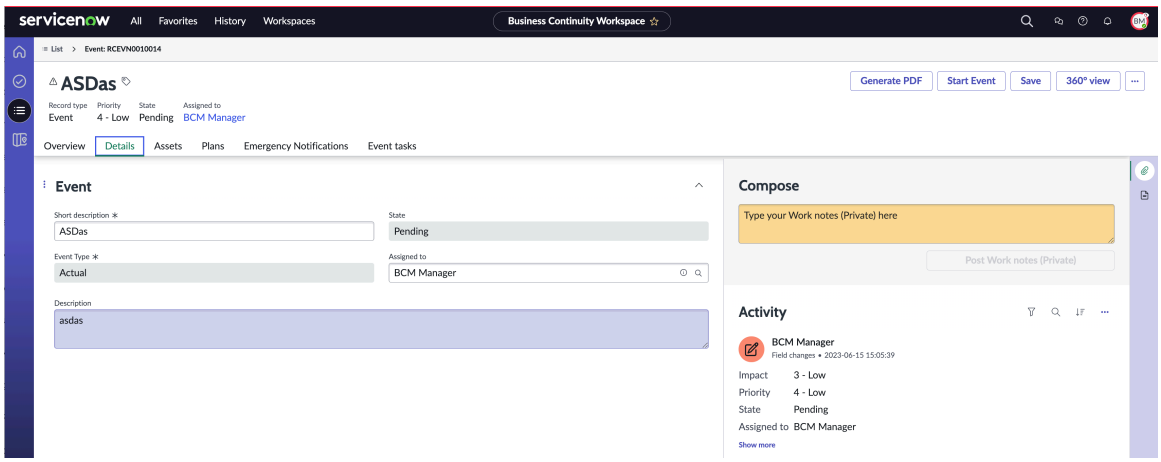
**Procedure**

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **crisis events** > **Pending** and select **New**.
   The **Create New Event** form is displayed.
3. In the **Details** tab of the **Create New Event** form, fill in the required fields.

   **Note:** For a crisis event, the event type is **Actual**.

   For more information on the fields, see Create Crisis Event form.

   A crisis event is created in the **Pending** state as shown in the following example.




   The state and details of the crisis event are displayed in the following tabs:

   - **Overview**: You can view the current state and overall state progression of the crisis event.
   - **Details**: You can view details on the crisis event such as its short description, state, event type, assignee, and so on.
   - **Assets**: You can select the impacted item type or the primary elements that you want to recover for an asset type.
   - **Plans**: You can add an ad-hoc plan for the selected asset to the crisis event.
   - **Emergency Notifications**: You can create a notification for the crisis event with the Everbridge integration.
   - **Event tasks**: You can add an ad-hoc task to the crisis event.
4. Select **Save**.
   The crisis event is saved in the **Pending** state and it is displayed in the Crisis events list view of the record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create Crisis Event form

Use the Create Crisis Event form in BCM UIB Workspace to add details about a crisis event.

## Create Crisis Event form

For a description of the field values, see the following table.

**Create Crisis Event form**

| Field | Description |
|---|---|
| Details tab | |
| Short description | Brief description about the crisis event. |
| State | State of the event. Defaults to the **Pending** state. |
| Event type | Type of the event. For a crisis event, the event type is **Actual**. |
| Assigned to | User or users from the Assignment group. If the **Assignment group** field is empty, then select any user. |
| Description | Description of the event. |

### Track the impacted assets and add a related plan

Track the impacted assets and add a related plan during a crisis event. You can monitor the assets and plans for the crisis event in BCM UIB Workspace. You can then recover your assets in the planning stage.

### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Crisis events** > **Pending** and select the crisis event in the list.
3. Select the **Assets** tab and select **Add**.

   You can add an asset that you want to recover during the crisis. The primary elements of the asset are listed as **Asset types**. The primary elements belong to the element definition type that is identified in the plan template. When you add an asset to the event, its associated dependencies are pulled into the event. The dependencies are displayed in the **Asset types** panel.

   **Note:** When you select **Add** for an application, all the dependencies that you had identified in the business impact analysis of that application are also added to the exercise.

4. In the Applications list, select the application and navigate to the **Plans** tab.
   When you add a plan to the crisis event, the related plans, assets, and event tasks that are associated with the plan also get pulled into the event.
5. Select **Add all plans related to asset**.
   If you have any plans related to the selected application in the instance, they are added to the exercise event.
6. Select **Save**.
   The crisis event is saved in the **Pending** state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Add a task to the crisis event

Add a task to the crisis event in BCM UIB Workspace. You can then monitor and complete the required actions to respond to the crisis event.

**Before you begin**
Role required: sn_bcm.planner, sn_bcm.program_manager

**Procedure**

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Crisis events** > **Pending** and select the crisis event in the list.
3. Select the **Event tasks** tab.

   **Note:** For the crisis events, the event type is **Actual**.

   When you add or update the plan to the crisis event, the related plans, assets, and event tasks that are associated with the plan also get pulled into the event.
4. To add an ad-hoc task to the event, select **New ad-hoc task**.

   **Note:** An ad-hoc task is added to the crisis event so that you can take corrective actions for the crisis event. When you add an ad-hoc task to the crisis event that is in the **Work in progress** state and if the activated plan is in the **Work in progress** state, the tasks will be in the **Open** state. If the activated plan is the **Pending** state, the task will be in the **Pending** state.

   For more information on the fields in the New Event Task form, see Create New Event Task form.

   **Note:** You cannot create an ad-hoc task for the activated plans that are in **Closed Complete** or **Closed Incomplete** state.

5. To start the crisis event, select **Start Event**.
   After you start the event, the event state is updated to **Work in Progress**.

   **Note:** If the event task has a circular dependency, you have to trigger the tasks manually for this event.

6. Select the first task and select **Trigger**.
7. Complete all the activated plans of the event tasks for the crisis event and select **Submit for Approval**.
8. To generate a PDF, select **Generate PDF**.
   If you have edit access to the crisis event, you can save a copy of the event in PDF format to your local hard drive.

   **Note:** By default, the PDF is generated and attached after the event is closed.

9. Navigate to the **Results** section on the **Details** tab and update the **Actual start** and **Actual end** dates for the event task.
10. Update the assignment fields, if necessary.
11. Enter any event task-related information in the **Work notes** field of the **Activity** section.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

12. Select **Save**.
13. Select the refresh icon ( ) to display the updated state of the asset or plan, and the actual time taken to recover the asset.

### Approve the crisis event

Approve the crisis event in BCM UIB Workspace.

**Before you begin**
Role required: sn_bcm.planner, sn_bcm.program_manager

**Procedure**

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Crisis events** > **Pending** and select the crisis event in the list.
3. Log in as the approver of the event and select the Event in the List view.
4. Select **Submit for approval**.
5. Select **Approve**.
6. Select **Save**.
7. Select **Closed Complete**.
   You can update the state of the event to **Closed Complete**.
8. Select **Closed Incomplete**.
   You can update the state of the event to **Closed Incomplete**.

## Structured workflows for Crisis map in BCM UIB Workspace

You can use the Crisis map interface in BCM UIB Workspace to receive alerts on possible threats for the business operations of your organization. You can then manage the alerts by initiating the response workflows.

Typically, the BCM program manager performs the following tasks to manage the alerts from the Crisis map interface:

- Manage the alerts in Crisis map. For more information, see Manage the alerts in Crisis map.
- Set controls in Crisis map to customize the alerts. For more information, see Set controls in Crisis map to customize the alerts.
- View resource layer clustering in Crisis map. For more information, see Select layer clustering in Crisis map.
- Monitor the assets within the impacted area in Crisis map. For more information, see Monitor the assets within the impacted area in Crisis map.
- Initiate response workflows for crisis management. For more information, see Initiate response workflows for crisis management.

## Additional information on Crisis map

- For information on the Crisis map view in BCM UIB Workspace, see Crisis map view.
- For information on the threats, feeds, and alerts in Crisis map, see Crisis map interface.
- For information on the administrative tasks in Crisis map, see Setup for Crisis map.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Manage the alerts in Crisis map

Manage the alerts from the Crisis map interface in BCM UIB Workspace. Then you can identify a threat and its geo-location from your asset location.

## Before you begin

Role required: sn_bcm.admin or sn_bcm.program_manager

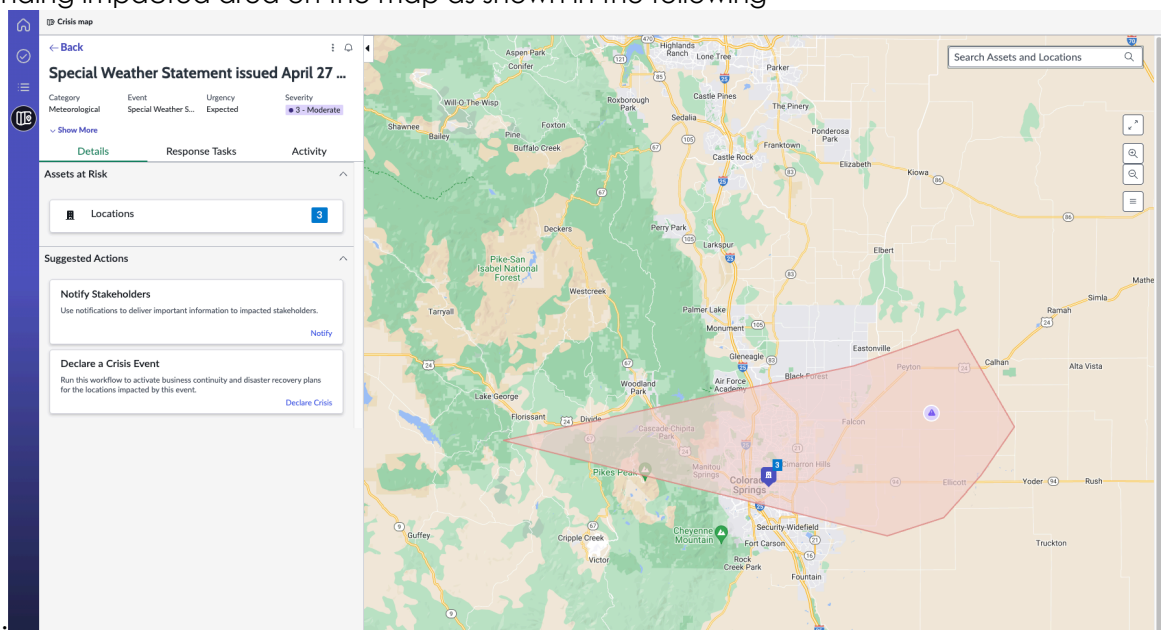
## Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, select the **Crisis map** icon.
3. Select an alert record.

   This action opens the alert record in the **Alerts** panel. You can view the details of the record in the header of the record.

   In the **Details** tab, you can view the assets at risk in the **Assets at Risk** section. You can view the suggested actions such as **Notify Stakeholders** or **Declare a Crisis Event** in the **Suggested Actions** section.

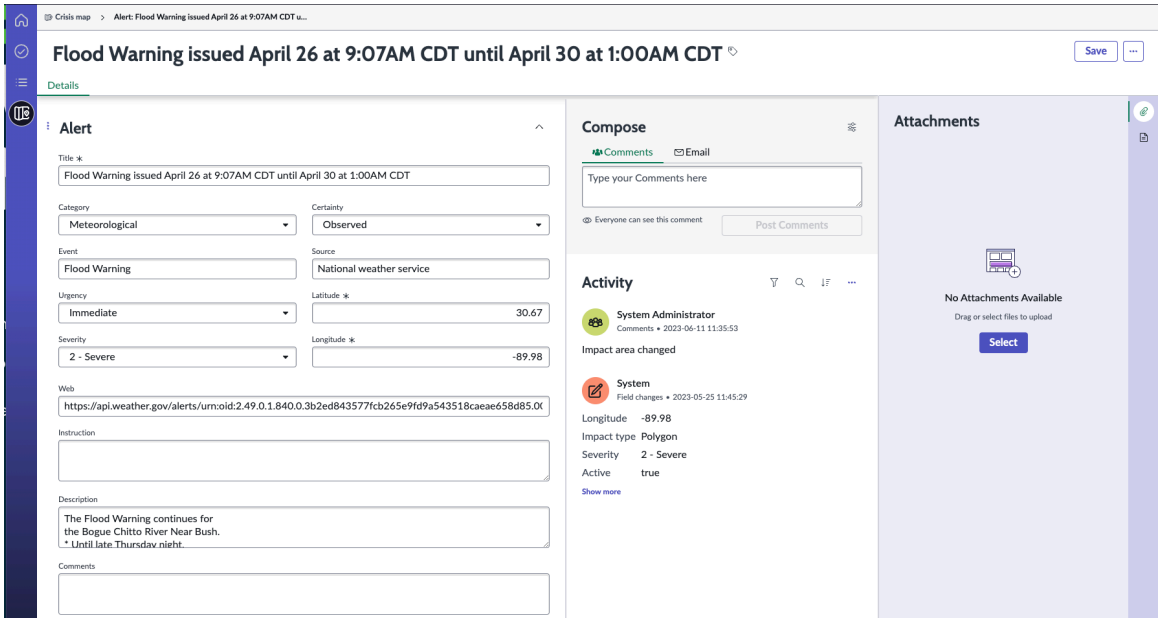
   You can open the detailed view of an alert and view its corresponding impacted area on the map as shown in the following example.




4. To open the alert details in the form view, select the **Open Alert** option in the **Alert menu** icon ( ⋮ ).

   This action opens the record on a separate **Details** tab as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




5. To view the response tasks that are associated with the alert, select the **Response Tasks** tab.
6. To view the activity on the alert and add your comments in the **Compose** section, select the **Activity** tab.
7. To dismiss an alert, select **Dismiss Alert** in the **Alert menu**.

   If the alert does not pose a threat currently to your employee locations, datacenters, core companies, or any of your business establishments, you can dismiss the alert. If you know that the alert would not hamper your business operations, you can dismiss it in the list view as well as in its detailed view.

   When you dismiss an alert in the list view, it is removed from the list. If you dismiss an alert from the detailed view, the alert is removed and brings you back to the list view so that you can review the other alerts in the list. In both cases, you can see a confirmation message about the dismissal of the alert.

8. To subscribe to the alert notifications, select **Subscribe** by selecting the bell icon in the Alerts panel.
   When an alert or its source feed item is updated, you receive the workspace notification.

### Set controls in Crisis map to customize the alerts

Set controls in the Crisis map interface in BCM UIB Workspace. You can then customize the alerts for assets, locations, and so on.

#### Before you begin

Role required: sn_bcm.admin or sn_bcm.program_manager

#### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, select **Crisis map**.

   The alerts section is on the left of the workspace and the map view is on the right.

3. Select the **Search assets and locations** search field in the map view on the right and enter the location or datacenter that is impacted by an alert.

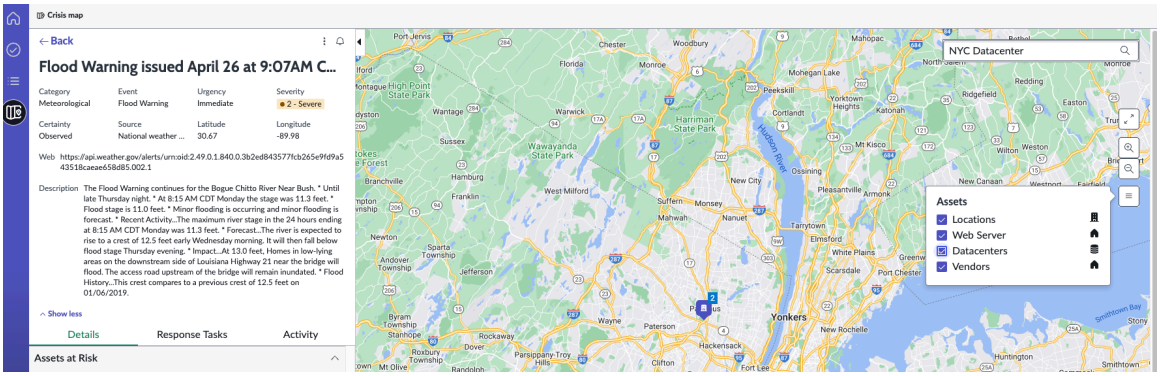
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When you search for a location, a mixed list of your company results with the display value of the records along with their icons, and the Google map pin icons appears.

If you are not sure of both the employee locations or datacenters, then use the Layers control.

4. To change the zoom level of the map and view specific areas, use the **zoom-in** and **zoom-out** control buttons.
5. To select and display the assets on the map, select the **Layers** icon.

   The assets such as **Locations**, **Web Servers**, **Datacenters**, or **Vendors** are displayed on the map as shown in the following example.




6. To clear the map of all the search results, select the **Reset** icon.

### Select layer clustering in Crisis map

Select resource layer clustering in Crisis map in BCM UIB Workspace. You can then view your assets or resources on the map.

### Before you begin

Role required: sn_bcm.admin or sn_bcm.program_manager

### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, select **Crisis map**.
3. Select the **Layers** icon.

   The layers on the map appear just as pins on a Google map and are configurable. All the layer details like the asset locations, assets, datacenters, and core companies are displayed on the map by their configured icons.

   Use the layers control to view only the selected or all assets that can be toggled on and off on the map. As a crisis manager, when viewing the active alerts you can make an informed decision by concentrating on a single asset that can be critical at that moment from the rest.

4. To display a selective resource or asset on the map, select the check box of that asset.

   The icons of the selected asset are displayed on the map. Layer icons are displayed within black borders, whereas alert icons are within a white circle.

5. Select an **Asset** icon on the map to view its details.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, if you select a datacenter icon that has no number or a count next to it, a pop over appears with the display information that you have configured in the Resource Configuration table [sn_fam_resource_config].

If you have configured the **Power** and **Power consumption** fields of the datacenter table [cmdb_co_datacenter] as the display fields in the Resource Configuration form, then the power consumption details of that datacenter are displayed on the pop over along with its location coordinates.

6. Select an **Asset** icon with a number next to it.

   The map zooms in to show all the assets that match with the count in that cluster. You can further select each asset within the cluster and drill down to any asset to view its details on the pop over.

   You can view only one pop-over at a time. When you select another node, the pop-over disappears.

7. Select the **Reset** icon in the map to clear the search results on the map.

### Monitor the assets within the impacted area in Crisis map

Monitor your assets that are at risk in Crisis map in BCM UIB Workspace, when an alert threat is observed near your business location. You can then protect your resources within the impacted area and prevent major loss for your organization.

#### Before you begin

Role required: sn_bcm.admin or sn_bcm.program_manager

#### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, select **Crisis map**.
3. Select an alert record to open the alert in its detailed view.

   You can see various details of the alert on the form header.

   - Title of the alert
   - Category of the alert
   - Urgency of the alert whether it is going to strike immediately or expected in future
   - Severity in terms of loss
   - Certainty as to how likely it can strike
   - Source of the alert feed
   - Coordinates of the impacted area
   - Source or the website from where the feed alert was received
   - Description

4. Expand the **Assets at Risk** section to view all the listed assets that are at risk.
   The **Assets at Risk** lists locations, datacenters, and core companies that lie within the impacted area of the alert. It also displays the count as to how many of these assets are impacted. You can view the impacted area on the map and take any of the suggested actions.

   The boundary of the impacted area for the alert on the map is marked in mauve color. You can view the assets that are at risk within this impacted area on the map. If one of

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

your location, datacenter, or a core company is impacted by the alert, you can edit the impacted zone to include the asset.

5. To edit an impacted area, select the **Alert menu** icon.

   a. Select the **Edit Impact Area** option.

   b. In the **Edit Impacted Area** pop over that opens on the map, select either **Custom Shape** or **Custom Radius** depending on the shape of the impacted area.

      - **Custom Shape**: Select **Custom Shape** if the impacted area is polygonal shape.
      - **Custom Radius**: Select **Custom Radius** if the impacted area is a circle.

   c. Select and drag the vertex on the boundary of the impacted area to include the asset location.

   d. Select **Save**.

6. Save or bookmark the URL of the alert to open the detailed view of the alert directly anytime.
7. In the **Assets at Risk** section, select an asset card like a location or datacenter.
   The list view of the records opens up in a new tab.
8. To view the details of the asset, select the link to the record in the **Name** column.
   You can view the complete details of the asset including its latitude and longitude.

### Initiate response workflows for crisis management

Initiate response workflows for your recovery teams in BCM UIB Workspace. You can then notify the stakeholders and help them respond to the threat and take necessary actions.

#### Before you begin

Role required: sn_bcm.admin or sn_bcm.program_manager

#### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, select **Crisis map**.
3. Select an alert record.

   While viewing the alerts and their severity, you can initiate appropriate actions and trigger Crisis Management workflows for the respective stakeholders to respond and act on the crisis. The **Suggested Actions** section lists various responses that you can initiate.

   Notify Stakeholders

   Notify important stakeholders of the assets that are at risk because of the alert.

   Declare a Crisis Event

   Start an event to activate the recovery tasks to recover the assets with a recovery team.

4. To notify a stakeholder of the impending crisis by an email, select the **Notify** button in the Notify Stakeholders card.
   In the modal window that opens, identify the concerned person or persons and communicate the information to them. It is a two-step process, where you identify the audience and draft an email to send it to them.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select an audience from the list in the Notify Stakeholders pop-up.
You can select an additional audience from the list whom you think must be notified too.

b. Select **Next**.

c. In the Step 2 of the process, verify the alert details and draft an email appropriately in the **Email Body** field.

d. Select the **Send Notification** button.
You get a message that the action is executed.

5. To activate a business continuity or disaster recovery plan for the locations that are impacted, select **Declare Crisis** in the Declare a Crisis Event card.
   a. Enter a brief description of the crisis event in the Declare a Crisis Event form that opens.
   b. Select **Next**.
   c. Select the assets at risk that are within the radius of the threat alert.
   d. Select **Start Crisis Event** button.

   When you trigger these actions, separate scripts run to trigger the alert notify action and the declaration of the crisis event. A message appears to confirm that your actions are executed. You can navigate to the **Response Tasks** tab to view the action and recovery event details.

   All the assets at risk are copied over to the Event Assets table [sn_recovery_event_asset] that is related to the event [sn_recovery_event].

### What to do next

1. If it is a recovery event, select anywhere on the **Response Tasks** card to take you to the event details.
2. In the **Details** tab of the event, update the details if necessary.
3. Select the **Start Event** button. The event for the crisis is then activated. All the associated plans for this recovery event and the tasks associated with it are set into action. The Crisis Management workflow begins to recover the impacted assets. For more information, see Crisis events.

   All the assets at risk are copied over to the Event Assets table [sn_recovery_event_asset] that is related to the event [sn_recovery_event].

## Sending notifications with Everbridge in BCM Configurable Workspace

You can send an emergency notification with Everbridge in BCM Configurable Workspace and inform the stakeholders about a crisis event.

Typically, the BCM program manager sends out the emergency notifications to the stakeholders. For more information on creating an emergency notification, see Create an emergency notification.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Additional information on Everbridge

- For information on the emergency notifications in Everbridge, see Emergency notifications in Everbridge notifications system.
- For information on the setup tasks for Everbridge, see Setup for Everbridge notifications.

## Workflow status of an emergency notification

When you send an emergency notification for a crisis event with Everbridge, it creates a corresponding incident along with a notification. You can track the notification delivery and monitor its status in Business Continuity Workspace until it is successfully delivered to the contacts from Everbridge.

## Status flow for an emergency notification

The status flow for an emergency notification lists different states of an emergency notification in Everbridge. The short description of the event in the Business Continuity Workspace is created as an incident with a notification in Everbridge.

Notification state

The emergency notification that is created and sent from the ServiceNow Business Continuity Management Workspace is tracked in the **Notification state** field.

Communication status

The emergency notification that is received in Everbridge and the different stages to which it moves until it is delivered are tracked in the **Communication status** field.

### Emergency notification workflow status

| Notification state | Communication status |
|---|---|
| **Draft**: The draft of the notification is stored in Business Continuity Workspace. | **None** |
| **Attempting to send**: The notification is being sent from Business Continuity Workspace. | **None** |
| **Error**: An error occurs in creating the notification in Everbridge. | **None** |
| **In Progress**: The notification is successfully created in Everbridge. | **Active**: A notification is created and is active.<br><br>An incident and a notification for the incident are created. The notification remains active for the duration set in Everbridge. |
| **Stopped** | **Stopped**: Notification is stopped from being sent. |
| **Sent** | **Sent**: After the set duration has elapsed, the state moves to Sent. |
| **Completed**: The notification is sent. | **Completed**: The state moves to Completed. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Create an emergency notification

Create an emergency notification in BCM UIB Workspace. You can then use Everbridge to notify the stakeholders.

### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager, or sn_bcm.admin

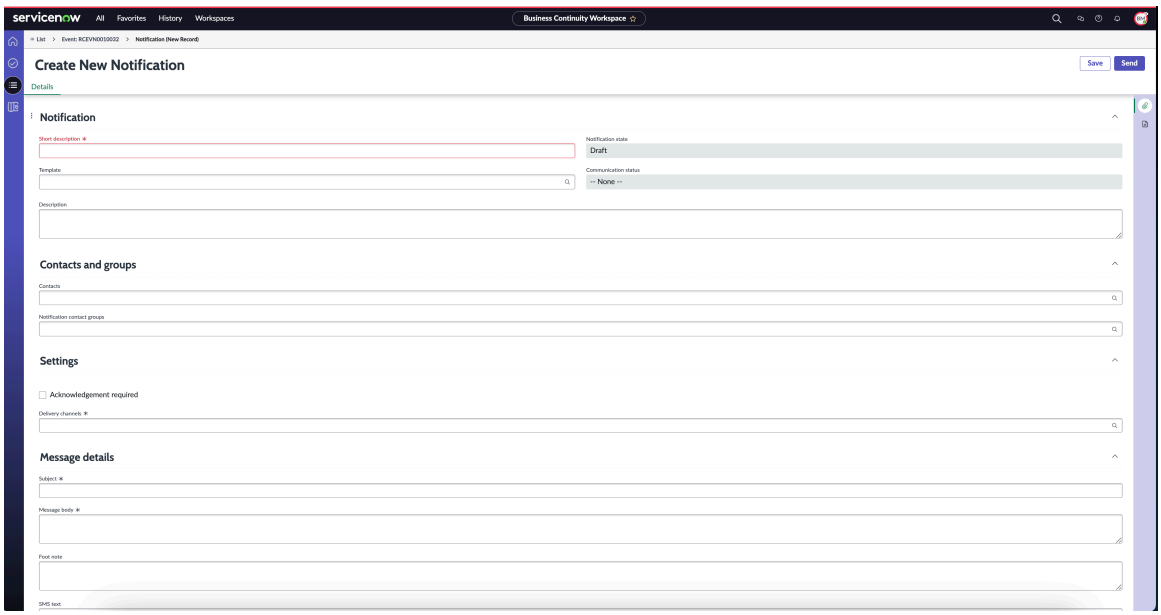
### Procedure

1. Navigate to **Workspaces** > **Business Continuity Workspace**.
2. In the List view, navigate to **Crisis events** in the **Pending** state.

   **Note:** If the **Exercise Method** is **Functional**, then you can create an emergency notification for an exercise event.

3. Select the link to the event record in the **Number** column.
4. Select the **Emergency Notifications** tab.
5. Select **New**.

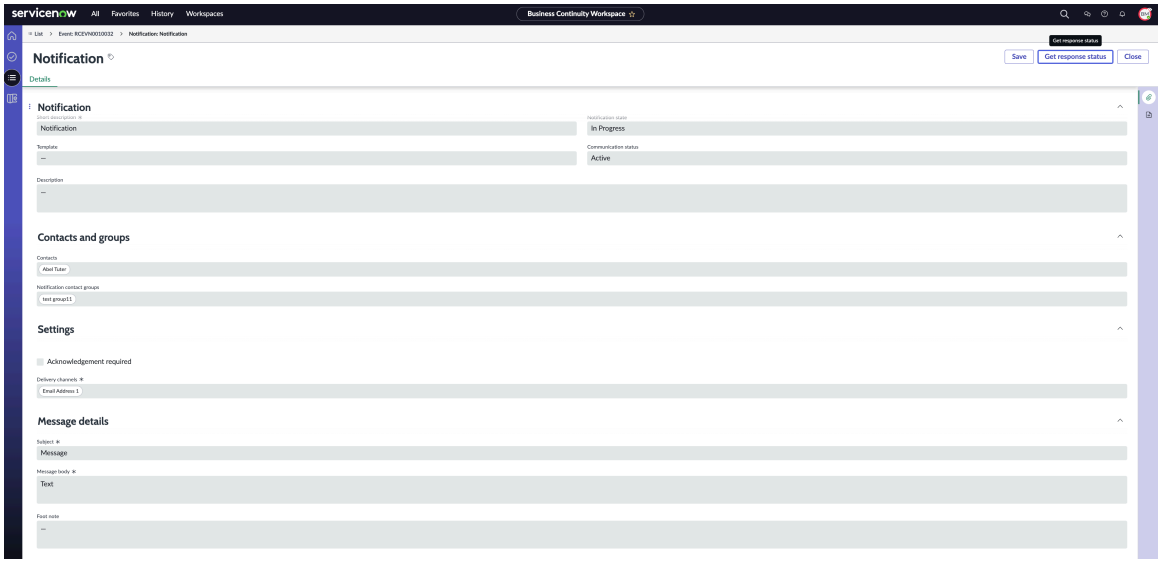
   The New Notification form is shown in the following example.




6. On the form, fill in the fields.
   For more information on the fields in the form, see Create New Notification form.
7. To save the notification and send it later, select **Save**.
8. Select **Send**.

   It creates a notification in Everbridge as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




When you create and send a notification for a crisis event in Business Continuity Workspace, a corresponding incident is created along with a notification in Everbridge.

9. To know if there are any errors in sending the notification, refresh the page.
   If the notification is not sent due to an error, the Notification state moves to **Error**.
10. To receive the state from Everbridge for the notification sent to the contacts in the **Communication status** field, select **Get response status**.

    Before you submit an event for approval, all the notifications that are **In Progress** must be closed.

    a. To delete a notification that is in **Draft** or **Error** state, select the link to the emergency notification record in the **Number** column.

    > **Note:** You cannot delete a notification that is in **Attempting to send**, **In Progress**, or **Completed** state.

    b. Select **Delete** in the **more** actions icon.

    > **Note:** Now that the event is closed and the corresponding incident in Everbridge is also closed, you cannot create any more notifications for this event.

11. Select **Save**.
    You can save the emergency notification.

### Create New Notification form

Use the Create New Notification form in BCM UIB Workspace to add details about an emergency notification.

#### Create New Notification form

| Field | Description |
|---|---|
| Short description | Title of the emergency notification |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Notification form (continued)**

| Field | Description |
|---|---|
| Template | Pre-configured template that has the subject of the mail and the delivery channels for the contacts. |
| Notification state | State of the notification in the ServiceNow workspace. |
| Communication status | State of the notification in Everbridge. |
| Description | Description of the notification. |
| Contacts and Groups | |
| Contacts | Persons to whom the notification is sent.<br><br>Contacts that are successfully synced with Everbridge are listed. |
| Notification contact groups | Groups of contact to whom the notification is sent.<br><br>Successfully synced contact groups are listed. |
| Settings | |
| Acknowledgement required | Option if an acknowledgement is required from the contact for the notification received. |
| Delivery channels | Communication channels that are used for sending the notification. |
| Message Details | |
| Subject | Title of the notification. |
| Message body | Introductory text message for the notification.<br><br>If a template is selected, then the message details are auto-populated from the template. |
| Foot note | Closing message for the notification. |
| SMS text | Text message sent through short message service (SMS). |

## Using BCM classic Workspace

This section provides information on managing the business continuity tasks in Business Continuity Management classic Workspace.

**Note:** Starting with the Utah release, the BCM classic Workspace is being prepared for future deprecation. It will be hidden from the navigation on the new instances but it will continue to be supported. The BCM UIB Workspace provides the latest experience for this functionality.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For information on managing your business continuity tasks in BCM UIB Workspace, see Managing business continuity workflow tasks in BCM UIB Workspace.

## Customizing the Business Continuity Management classic Workspace

You can set up the basic settings and features in the Business Continuity Management classic Workspace for your specific requirements.

**Note:** The BCM classic Workspace is being prepared for future deprecation. It will be hidden from the navigation on the new instances but it will continue to be supported. The BCM UIB Workspace provides the latest experience for this functionality.

For information on how to configure commonly used custom components in BCM classic Workspace, see the KB1442692 article.

**Note:** You must log in to Now Support to view the Knowledge Base articles.

## Migrating reports and custom changes to BCM UIB Workspace

If you are an existing customer of the Business Continuity Management application and you have customized UI actions, you must migrate those actions to BCM UIB Workspace.

**Note:** The BCM classic Workspace is being prepared for future deprecation. It will be hidden from the navigation on the new instances but it will continue to be supported. The BCM UIB Workspace provides the latest experience for this functionality.

The UI actions that were shipped with the Business Continuity Management application have been migrated to the BCM UIB Workspace as part of the Business Continuity Management application software.

If you have customized few UI actions for your specific requirements, you must migrate them manually to the Business Continuity Management UI Builder Workspace.

For information on how to migrate the UI actions, see the KB1444397 article.

## Structured workflows for Business Impact Analysis

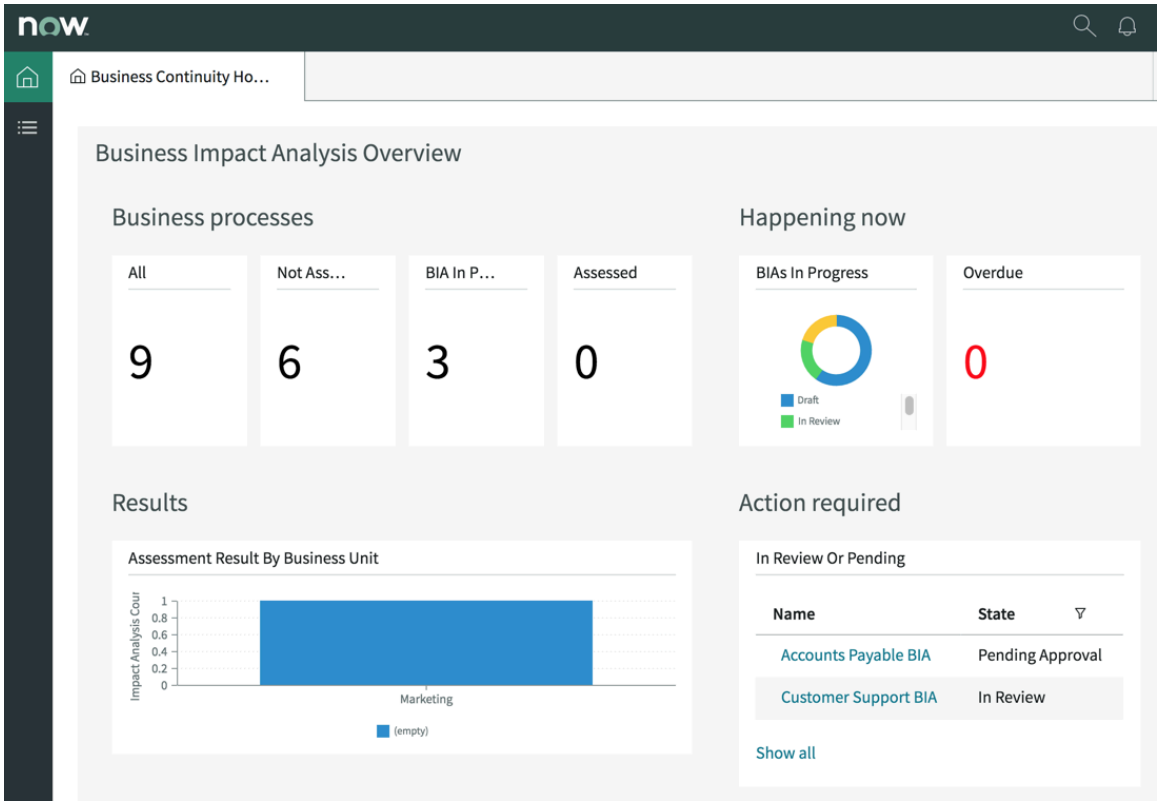
Business impact analysis helps you to predict the consequences of a disruption on a business process or business function.

A business process is a set of tasks done by a business organization to deliver a business service or product to customers. When a business process in disrupted, the impact to the organization can be huge in terms of revenue and reputation. Business impact analysis (BIA) is performed to identify and prioritize critical processes, quantify or qualify the impacts, and identify recovery dependencies. Ideally, business impact analysis on critical processes must be performed annually.

The assessment of a business critical process disruption helps you to estimate the consequential impact on your business revenue, legal issues, workforce disruption, or business reputation. It also enables you to identify the dependencies of your business process on business applications, technology, or vendors that might be affected. This analysis gathers the information needed to develop recovery strategies.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

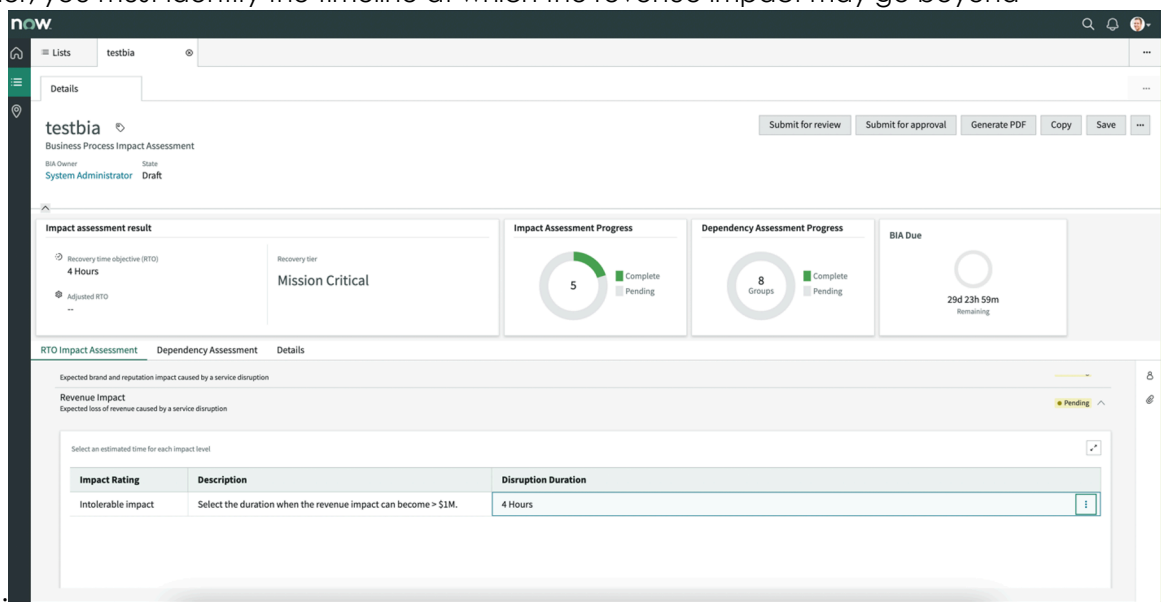
### Business impact analysis overview




## Impact ratings for your business impact analysis

The Business Continuity Management (BCM) administrator of your organization defines the impact ratings for your business impact analysis (BIA) and decides if the impact is tolerable for your business process. For more information on the impact ratings, see . According to the configuration set up by the BCM administrator, the questions are displayed in the **RTO Impact Assessment** tab.

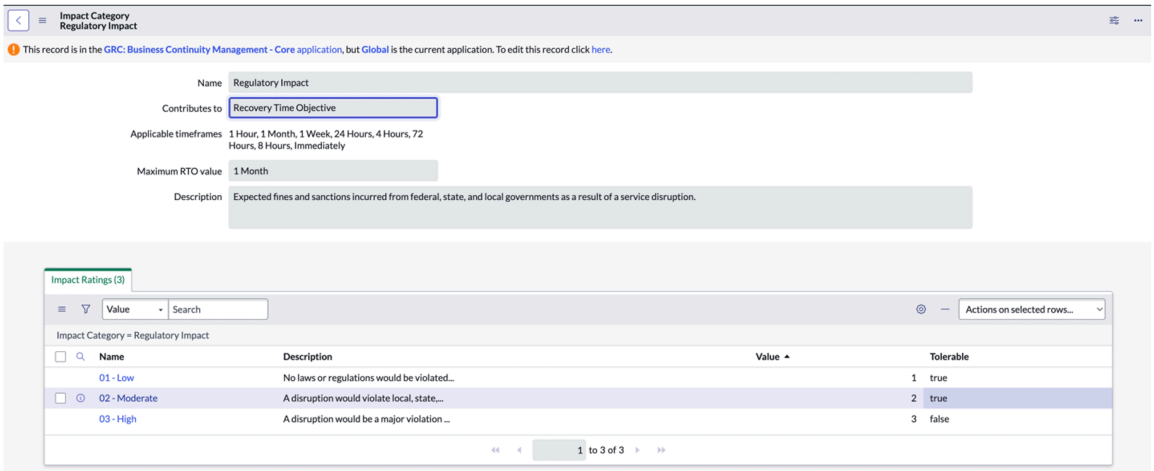
Consider the following example where the BCM administrator has configured an intolerable impact rating for the Revenue impact category. The BCM administrator has defined what qualifies to be an intolerable impact. As a BIA owner, you must identify the timeline at which the revenue impact may go beyond $1M.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Multiple impact ratings for an impact category

If your BCM administrator has configured the assessment questionnaire to include multiple impact ratings for an impact category, the impact category ratings are displayed in the Impact Category view as shown in the following example.




The BCM administrator can specify a threshold of non-tolerance for the impact ratings, per impact category. The disruption duration for the first non-tolerable impact category is selected for the recovery time objective (RTO). The impact ratings have the following specified values:

- Low = 1
- Moderate = 2
- High = 3

See the following example for the sample RTO calculation.

### Example to show the calculation of impact category

**Regulatory Impact**

Expected fines and sanctions incurred from federal, state, and local governments as a result of a service disruption.

| Impact Rating | Description | Disruption Duration |
|---|---|---|
| 01 - Low | No laws or regulatio... | 4 Hours |
| 02 - Moderate | A disruption would v... | 24 Hours |
| 03 - High | A disruption would ... | 72 Hours |

### Sample RTO calculation

| Scenario | Non-tolerable impact | Description |
|---|---|---|
| Scenario 1 | In the Impact Ratings table, the **Tolerable** field is set to **false**. | If the administrator has specified that Low regulatory |

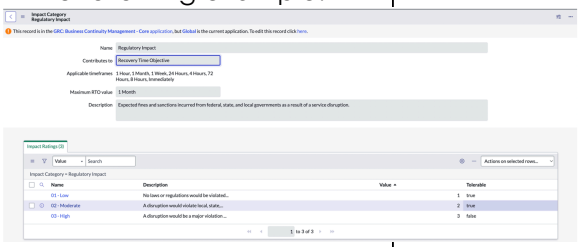
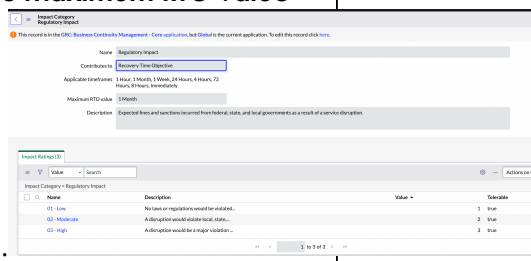
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Sample RTO calculation (continued)**

| Scenario | Non-tolerable impact | Description |
|---|---|---|
| | | impact is non-tolerable, its corresponding disruption duration is set as the recovery time objective (RTO).<br><br>In this example, the disruption duration for the **01 - Low** impact rating is set to 4 hours. Therefore, the recovery time objective (RTO) for the impact category is above 4 hours.<br><br>Even if the moderate impact disruption duration is shorter, the calculation will select the value from the first alphanumerically sorted impact rating that has the **Tolerable** field set to **false**. |
| Scenario 2 | In the Impact Ratings table, the **Tolerable** field is set to **false**. | If the administrator has specified that Moderate regulatory impact is non-tolerable, its corresponding disruption duration is set as the recovery time objective (RTO).<br><br>In this example, the disruption duration for **02 - Moderate** impact is set to 24 hours. Therefore, the recovery time objective (RTO) for the impact category is above 24 hours. |
| Scenario 3 | In the Impact Ratings table, the **Tolerable** field is set to **false**. | If the administrator has specified that High regulatory impact is non-tolerable, its corresponding disruption duration is set as the recovery time objective (RTO) as shown |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Sample RTO calculation (continued)**

| Scenario | Non-tolerable impact | Description |
|---|---|---|
| | | in the following example.<br>  <br>In the tabular example, the disruption duration for **03 - High** impact is set to 72 hours. Therefore, the recovery time objective for the impact category is above 72 hours. |
| Scenario 4 | The **Tolerable** field for the Low, Moderate, and High impact ratings is set to **true**. | If the administrator has set all the impact ratings as tolerable, the value specified in the **Maximum RTO value** field in the template is selected as the recovery time objective (RTO).<br><br>In the following example, the administrator has set all the impact ratings as tolerable. Therefore, the recovery time objective (RTO) is one month as per the value specified in the **Maximum RTO value** field.<br>  |

Calculation of category score from impact analysis questions for an impact category that contributes to Recovery Point Objective (RPO)

If the impact category contributes to **RPO**, then evaluate each impact analysis question in that RPO category based on the value of your data like business critical, operation critical, business essential, or operation essential. The maximum value among all the questions of that RPO is considered as the Category Score of that Impact Category and stored in the Impact Category Results table [sn_bia_category_result].

Calculation of overall impact assessment result for a BIA

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When you update the **Disruption Duration** of an impact category, the RTO of the BIA is automatically updated. The RTO of the BIA is set as the lowest tolerable downtime from each impact category.

For example, consider a BIA having four impact categories – Legal, Reputation, Workforce, and Regulatory. When you update the disruption duration value of the legal impact category, then the RTO value of the BIA is recalculated based on the lowest tolerable disruption duration from each impact category. The Recovery Tier varies from organization to organization and is set based on the recalculated RTO value.

| RTO value | Recovery Tier |
|---|---|
| Immediate | Mission Critical |
| 1 Hour | Mission Critical |
| 4 Hours | Mission Critical |
| 8 Hours | Business Critical |
| 24 Hours | Business Critical |
| 72 Hours | Essential |
| 1 Week | Essential |
| 2 Weeks | Non-Essential |
| 1 Month | Non-Essential |

### Create a business impact analysis

Create a business impact analysis (BIA) to get the necessary information for a plan. Use the BIA to identify the recovery time objective for an item and prioritize assets that have most and least critical dependencies. Use the information to establish their recovery strategies during the planning phase.

## Before you begin

Role required: sn_bcm.program_manager or sn_bcm.planner

## Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click **Start a BIA** in the **Actions** section.
3. On the form, fill in the fields.

**Start a BIA form**

| Field | Description |
|---|---|
| Name | Name of the business impact analysis.<br><br>Describe the BIA within 255 characters length. |
| Template | Template that you can use as a model to create the BIA.<br><br>The template BIA has the primary elements (applications, business processes, and |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | locations), impact categories, and the dependent assets identified for the type of assessment. |
| Applies to table | Table that stores the template's primary element data. |
| Applies to | Business process, business application, or any other asset that is assessed in the BIA. |
| Business Unit | Business unit that uses the business process and for which the BIA is assessed. |
| Department | Department which uses the business process. |
| BIA Owner | Person who owns and is responsible for completing the BIA. BCM lead can review the BIA. |

4. Click **Submit**.

A BIA is created in **In Draft** state.

State transitions for a BIA:

In Draft

It is the state where your BIA is under edit. Add RTO, RPO, and dependency assessments. Either you can submit the BIA for review, in which case ensure that a BCM Lead is assigned to the BIA. Or, as a BIA owner you can submit the BIA for approval.

In Review

Review the BIA and submit it for approval. In this state, the BCM admin can modify the BIA owner and BCM lead.

Pending Approval

When you click **Submit for Approval**, the BIA is set to **Pending Approval** state. The approval configurations, approval levels, and approval rules are evaluated against the BIA to determine the approvers. If there are no approval records in the requested state for the BIA, then as a BCM program manager you can either **Reject** or **Approve**. You must add RTO, RPO, and dependency assessments before you submit for approval. In pending approval state, the BIA is read only and the RTO, RPO, and dependency assessment details cannot be modified. The state of the plan and its related tables becomes read only.

Returned

BIA is editable. BCM admin can change the BIA owner in this state. When the BIA is rejected, it is set to **Returned** state.

Approved

When a BIA is in an approved state, it becomes read only and the RTO, RPO, and dependency assessment details cannot be modified. Your only option to change the status is to move it to **Archived** state.

Archived

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the BIA is archived, it becomes read only. All the underlying tables like impact dependency groups, impact category results, and dependencies from where the BIA retrieves data to populate in the impact assessment and dependency assessment tabs become read only. You can no longer edit the information in these tabs. In this state, you can also generate a PDF of the BIA.

**Note:** A scheduled job runs weekly to move the BIAs that have expired to **Archived** state.

### Assess impact categories and dependencies of a business process

Assess the different components of a business impact analysis (BIA). First by assessing and determining the impact categories of a business process. Second, by identifying any underlying dependencies that the business process requires across different dependency types.

### Before you begin

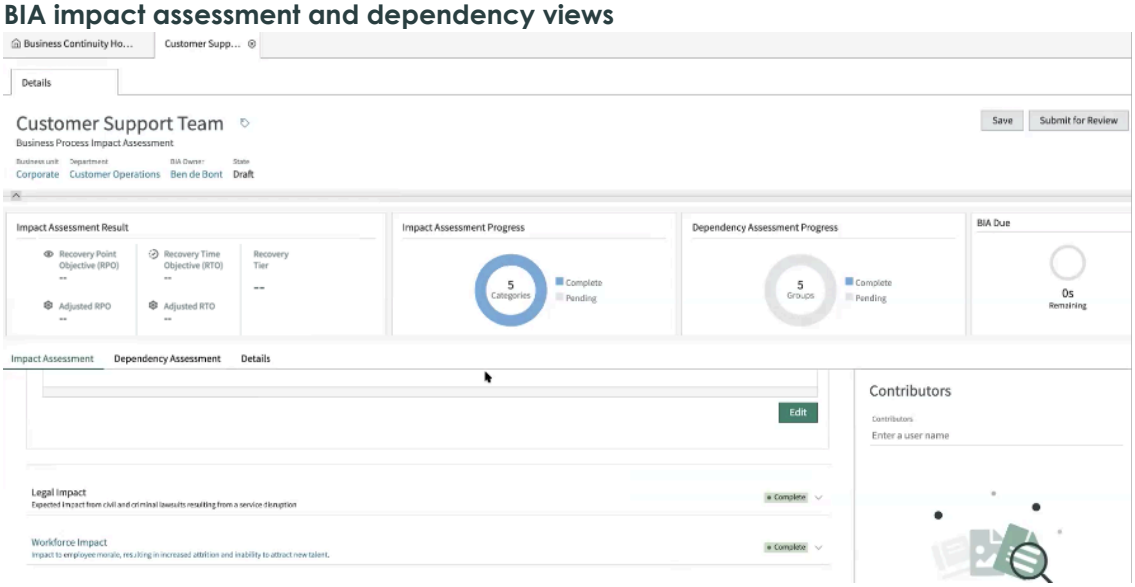
Role required: sn_bcm.program_manager or sn_bcm.planner

### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon ( ).
   By default the records in the **In Draft** state of the Business Impact Analysis list opens.
3. To create a business impact analysis (BIA) record, click **New**.
4. To update an existing BIA, click the link to the record in the **Name** column.

   You can view different cards that give the information on the impact assessment result, its progress, and the dependencies of the business process on business application, hardware, software, or vendors.

#### BIA impact assessment and dependency views




Impact Assessment Result

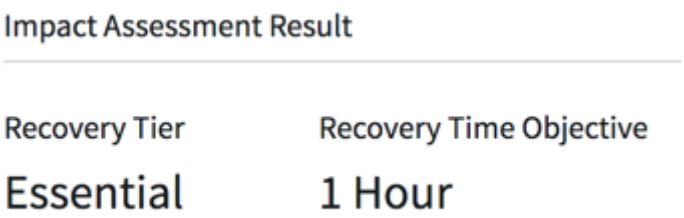
This card provides the assessment results of the recovery tier level and the recovery time objective for the item that is assessed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Recovery Point Objective** (RPO): Metric that evaluates the data loss during the business disruption duration that can exceed the tolerance level. RPO results appear in the Impact Assessment Result card only when the primary element assessed in the BIA requires data backup. Otherwise the card shows only the Recovery Time Objective (RTO) and recovery tier results.
- **Recovery Time Objective**: Metric that calculates how quickly the business must recover an element or an item after a disruption. RTO is measured in terms of how long your business can survive following a disaster before operations are restored to normalcy. If the RTO is four hours and the item recovered is beyond four hours, then your business could suffer quite some loss.
- **Recovery Tier**: Organizations differ in defining recovery tiers depending on the item and the time by which it should be recovered on the state of a crisis. A recovery time objective of **Immediately**, **1 hour**, or **4 hours** is impending and falls within the **Mission Critical** recovery tier level. On the other hand, an RTO of two weeks to one month can be graded as a **Non-Essential** recovery tier, which may not incur considerable loss to the business.

**Note:** You can configure the mapping of recovery tiers to RTOs as per your requirement.

**Impact assessment result**




Impact Assessment Progress

This component indicates the categories of impact that you have assessed and completed in relation to the categories that are assessment pending. As you complete the assessment for each category of impact, you can see the progress of the **Impact Assessment Progress** ribbon component. The color-coded ribbon component prompts you to complete the assessment for the pending impact categories.

**Impact assessment progress component**




Dependent Assessment Progress

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Identifies the dependency of the business process on different asset classes or types for its functioning. The assessment identifies the relationship between the business process and the business application, software, workplaces, or vendors. Or, the asset types that the process uses. The progress of the dependency assessment pie chart advances as you complete assessing the business applications, software or hardware, and vendors that the business process depends on.

**Dependency assessment progress pie chart**




BIA SLA

The business impact analysis also requires a specific time by which the assessment of a business process must be completed. By default, the SLA timer is set to 30 days and it marks the time since the BIA is drafted, which is **In Draft** state, until the time it is complete, which is **Approved** state.

5. To assess the different types of business impact categories on the business process, click the **RTO Impact Assessment** tab.
   All impact categories are configurable. A business process draws a set of impact categories, by default, from the template that you have used for the business impact analysis. For more information, see: Review an impact category and assess its downtime.
6. To answer questions on the data value of the asset in terms of its impact on the business and its data change frequency, click **RPO Impact Assessment** tab.
   For more information, see Assess RPO impact of technology assets on the business.
7. To review the dependency groups and identify the items within each group that your business process depends on, click the **Dependency Assessment** tab.
   You can prioritize your business continuity and recovery plans based on the criticality of the assets that your business process utilizes. For more information, see: Identify dependent items to prioritize recovery plans.

Order of impact categories

The order in which the impact categories appear in the **RTO Impact Assessment**, **RPO Impact Assessment**, and **Dependency Assessment** tabs depend on the order in which the impact categories are created in the template that is used in the BIA.

The order of impact rating in the RTO impact assessment grid and the order of the questions in the RPO impact assessment grid are defined by the impact rating scale and the impact analysis questions in the BIA, respectively.

However, any user who can access the BIA can change the order of the RPO impact grid, RTO impact categories, and dependency groups.

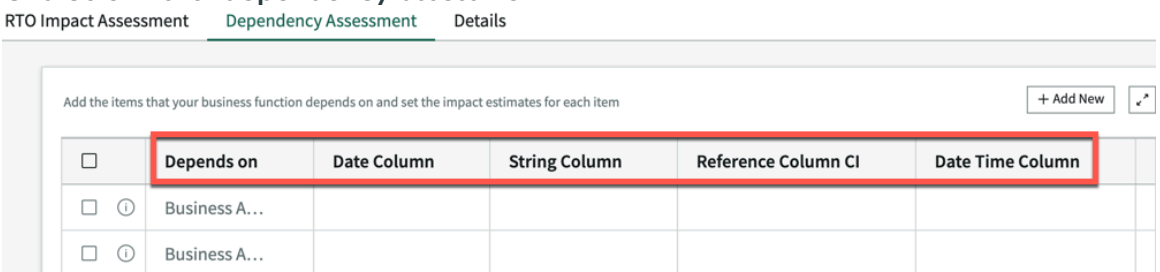
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Columns in dependency group grid

If you had set up column configurations for an element of a dependency group and enabled your grid configuration as active, then you can view those columns in the dependency grid for the corresponding dependency group in which element definition matches with the grid configuration element definition.

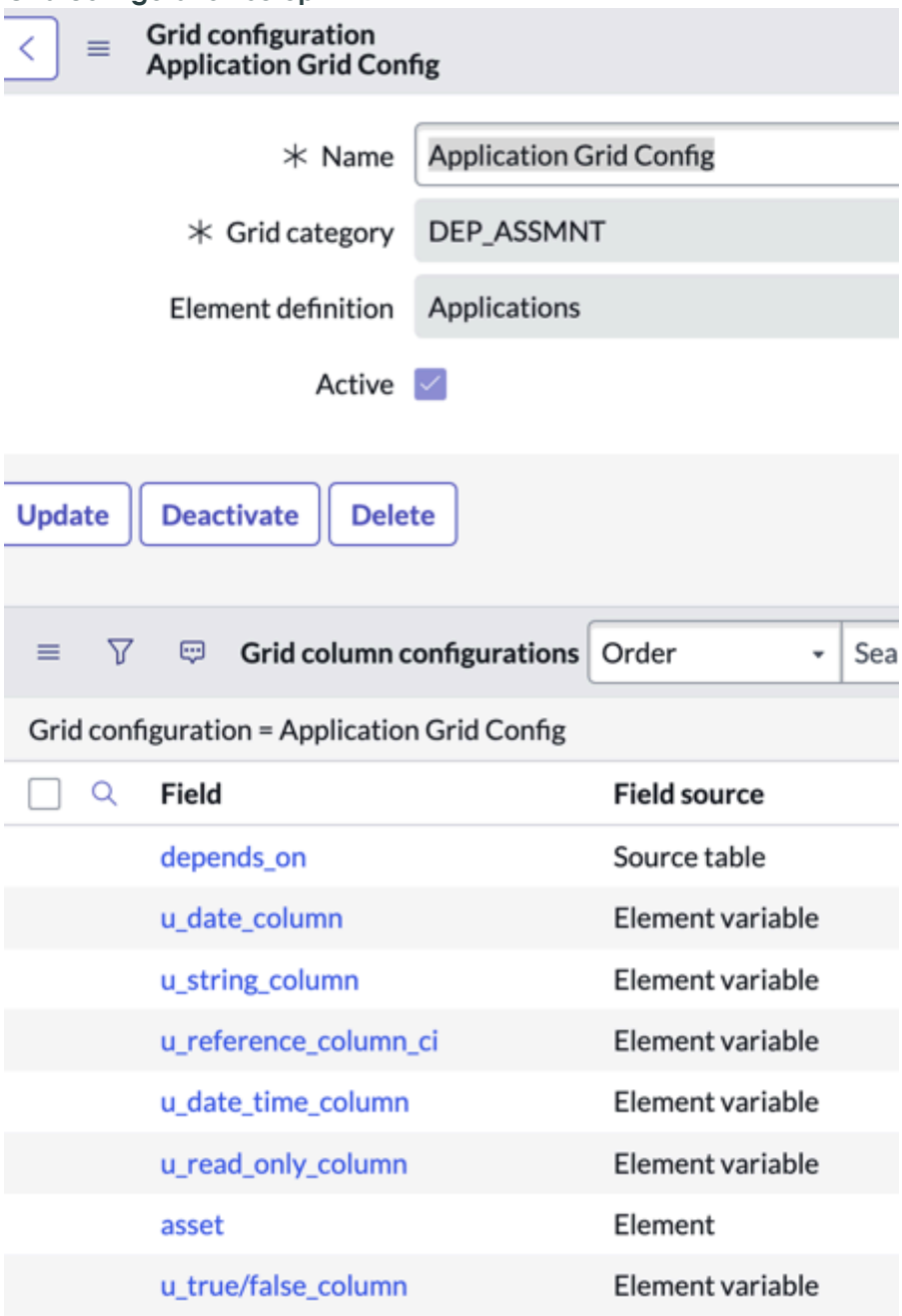
Otherwise, you can view the grid that is rendered based on the configured view; that is either IT asset or non-IT asset view based on the required data backup value of the dependency group.

**Grid columns for dependency assessment**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Grid configuration setup**




For ad hoc reporting of variables created for dependency: Add the columns in Dependency report source [sn_bia_dependency_report_source] table to match the variables that you defined in Element variable where the **Enable reporting** option is set to **true**. A scheduled job that runs weekly:

- retrieves the
  - dependencies (sn_bia_dependency), where the impact analysis is in approved state, updated in the last seven days, and has not expired, and the
  - corresponding element
- and updates the data in the reporting table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To display the columns that you require you must set up the element variable and grid configuration. For more information, see, Grid configuration for column display.

8. To change the order of appearance of the impact categories in RTO, RPO, and dependency groups in dependency assessment, navigate to **Business Continuity** > **Business Impact Analysis** > **Impact Category Results**.
   a. Click the impact analysis record.
   b. To change the order of the impact categories for RTO and RPO, click the Impact Category Results related list and change the order in the **Order** column.
   c. To change the order of dependency groups, click the Impact Dependency Groups related list and change the order.

### Review an impact category and assess its recovery time

Review the impact categories and define the timeframe during which the organization would experience the downtime of its business processes. Analyze the downtime or disruption duration, which helps to determine the recovery time objective for the asset that is assessed.

### Before you begin

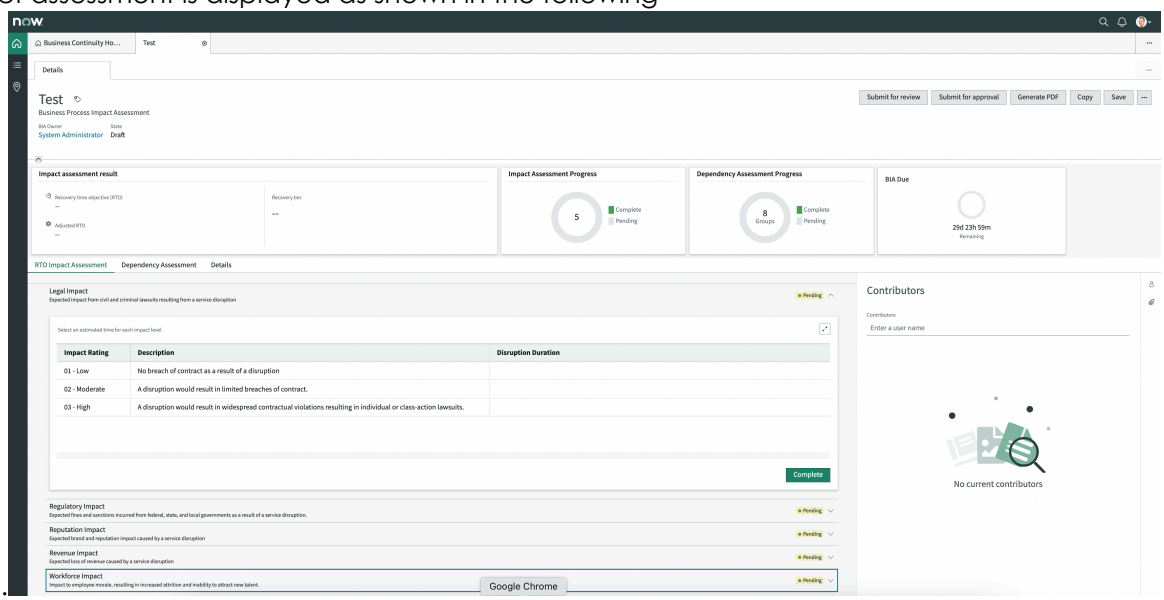
Role required: sn_bcm.planner, sn_bcm.program_manager

### About this task

The BCM administrator configures the impact categories that are relevant to your business. For more information on configuring an impact category in the classic BCM workspace, see and Structured workflows for Business Impact Analysis.

### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Select the lists icon ( ).
3. In the **Name** column, select the link to the BIA record that is in the **In Draft** state.
   An impact assessment is displayed as shown in the following example.




4. To update a business impact category with its recovery time, select the **RTO Impact Assessment** tab.
   The state of the impact category changes to **Pending** and the grid is editable.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Double-click the **Disruption Duration** cell for each Impact rating.

   Disruption duration is an estimated duration of the disruption that is based on your responses to the assessment questions and your subject matter expertise. If you're the BIA owner, you have to select the right disruption duration based on your responses to the assessment questions and your subject matter expertise. The disruption duration is used for calculating the recovery time objective (RTO).

6. Select the duration from the list that pops up depending on the criticality of the impact.

   The system prompts you to complete entering the disruption duration for all impact ratings of an impact category.

   The list of values displays only those durations that are configured as applicable timeframes for the recovery time objective (RTO) type impact category.

7. Select the **Disruption Duration** cell of the next Impact Rating to enter its value and save similarly.
8. Select the **Complete** button after you've assessed the duration for all impact ratings of an impact category.
   The state changes to **Complete** and is closed for editing unless you select the **Edit** button again.

### Assess RPO impact of technology assets on the business

Use the RPO impact assessment tab to enter asset information. The information can be critical from the objective of its recovery, the data value of the asset, and the frequency at which the data changes in the asset.

#### Before you begin

Role required: sn_bcm.program_manager or sn_bcm.planner

#### About this task

Not all elements require data backup, however technology assets like IT hardware and software require data backup due to the critical information content.

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon ( ).
   By default the records in the **In Draft** state of the Business Impact Analysis list opens.
3. To create a business impact analysis (BIA) record, click **New**.
4. To update an existing BIA, click the link to the record in the **Name** column.
5. To assess a BIA of its recovery point objective, click the **RPO Impact Assessment** tab.
   The **RPO Impact Assessment** tab appears only if you, as a BCM administrator, had set the **Requires data backup** field as **Yes** in the .
6. Enter the data value of the asset in terms of its RPO impact on the business in the **Response** cell of the Data Value grid.
7. Click **Complete**.
8. To mention the frequency at which the data changes in the asset, enter your response to the questions in the Data Change Frequency grid.
9. Click **Complete** after you answer all the RPO related questions.

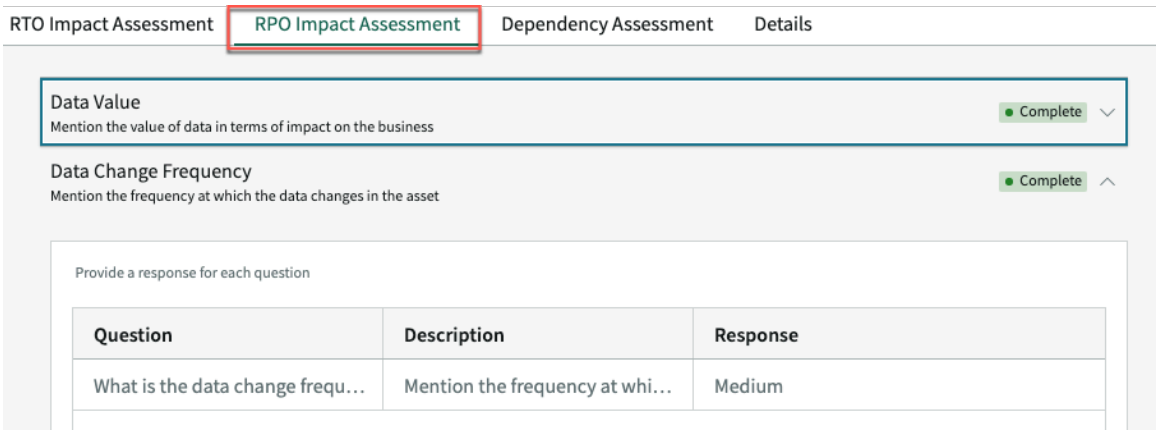
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Result**
Calculation of **Recovery Point Objective (RPO)** for **Impact Assessment Result**

If the impact category contributes to RPO, then the RPO calculation is as follows:

RPO depends on the rating or the response that you give for each question in the impact category of RPO Impact Assessment.

**RPO assessment result**

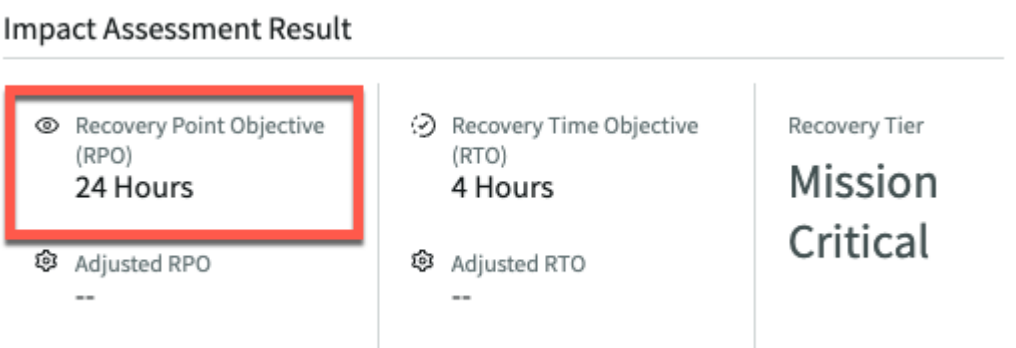



Based on your response that you have selected for each Impact analysis question of an impact category, the system calculates the RPO.

For example, if two questions have a Medium (value is 20) response and one question has High (value is 30) as response, then the system considers the response whose value is maximum. Hence, in this case the impact rating is considered as High and the value is 30.

The impact rating has an integer value preconfigured in the Impact Rating table [sn_bcm_impact_rating]. This value is updated as the **Category score** for the corresponding impact category in the Impact Category Results table [sn_bia_category_result]. The system picks up the maximum category score across all impact categories. This score falls within a range of lower and upper threshold values. The threshold range within which the maximum score falls corresponds to a timeframe, which is stamped as **Recovery Point Objective (RPO)** in the **Impact Assessment Result** card of the BIA.

**RPO value in Impact Assessment Result card**




The mapping results of the threshold score and the timeframe are stored in the Score timeframe mapping table [sn_bia_score_timeframe_mapping].

### Identify critical dependencies to prioritize recovery plans

Use the **Dependency Assessment** tab to identify items or assets that belong to a definite object type or a dependency group.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_bcm.planner, sn_bcm.program_manager

### About this task
Add a description of use and a timeframe to recover the item and provide data backup for the item. Assessing dependencies for a group helps you to know the underlying dependent items or assets of your business process. This assessment helps to prioritize critical dependencies that require recovery strategies to be established during the planning phase.

The BIA template that you use to create a business impact analysis has dependency groups associated to it. When you do an assessment, the dependency groups are automatically populated in the BIA. You can view them as Applications, Hardware, Software, Vendors, Workplaces, and others, each in its own container depending on how many of these groups are associated to the template. Each of them is a dependency group and you can add or remove items that belong to each group within its container.

**Note:** You can add or remove dependent items only if you are a user with appropriate access.

### Procedure
1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon  ).
3. Click the link to the record in the **Name** column in the **In Draft** state.
4. To review a group and identify the items within each group, click the **Dependency Assessment** tab.
   You can click the container to know the group and the items that belong to the group. For example, if the group is Application, you can select an item related to the business process that is assessed like Enterprise Resource Planning or Customer Relationship Management.
5. To add an item to a dependency group, click the **Add New** button of that container.
   - If it is the Application, Hardware, or Software dependency group that uses class extensions to populate configuration items and discover technologies or software, see Add dependencies based on CI relationships in CMDB.
   - If it is Vendors or Locations group, add assets accordingly. You can add multiple items in the modal form. The grid in the container becomes editable and you can enter data in each cell for an item.

   The state of the dependency group changes to **Pending**.

   a. Select an item from the list in the **Depends on** cell.

   b. Double-click the **Description of Use** cell and enter the function or role of the item.

   c. Select the time period in the **Required Recovery Timeframe** cell by which the item is to be recovered.

   d. In the **Required Data Backup** cell, select the time period by which a data backup for the asset can be provided.
   While configuring an element in the Element Definition form, you can set the **Requires data backup** field as **Yes**. However, at the time when a BIA is created, the application copies the required data backup information from the element definition over to the dependency group of the BIA. If at this point, the required data backup is true for the dependency group, then the **Required Data Backup** column appears in the grid.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. To expand the dependency grid to full screen and edit the grid values, click the full screen icon ( ).
   You can use the collapse screen icon ( ) to collapse the grid back to the normal screen size.
7. To update a group with dependent items, click the **Edit** button.
   The state of the dependency group changes to **Pending**.
8. To remove a previously identified dependency item, select the item in the check box and click the **Remove** button.
   When you click **Remove**, the record is deleted from the Dependency table [sn_bia_dependency].
9. Click **Complete** to complete the assessment of a group.
   Ensure that you have entered data in all the cells for the items before clicking complete. Otherwise, the system prompts you to fill in the incomplete cells. The container closes, the state is set to **Complete**, and you are directed to the next container. You cannot edit it unless you click the **Edit** button again.
10. Click **Save** to save the BIA and its dependency details.
11. Click **Submit for Review** to submit the BIA for a BCM program manager's review.
12. Click **Add Dependencies** to add dependent CIs collectively for all the dependency sections of the BIA.
    If the dependency groups depend on configuration items (CIs) in CMDB, then those CIs are linked as dependent items for the corresponding group in each section.

    **Note:** Dependency mapping of the dependency groups to their CIs is tracked up to five levels. Items within these five layers are added as dependent items to those Dependency Assessments that are only defined in the BIA template. For example, if Applications, Hardware, and Software are defined as Dependency Assessments in the Business Process BIA template, then only those CIs mapped up to five levels of the Dependency Assessments are added.

    To select and add CI as dependent item to each dependency group individually, see Add dependencies based on CI relationships in CMDB.

### Add dependencies based on CI relationships in CMDB

Add an item by referencing its CI relationship to drill down to the item that is related directly to the dependency group. You can map the item's relationship with the dependency group while assessing the business impact analysis of an asset that is at risk.

#### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager

#### About this task

If it is an Application, Hardware, or Software dependency group that uses class extensions to populate configuration items and discover technologies or software, you can add items by filtering records based on the item's relationship with the BIA dependency group. Or, you can add items to the group by simply selecting items from all the records.

For example, your business function, Accounts Receivable, may depend on the business application, Acrobat, to complete a business process. Therefore, the relationship is captured as Depends on::Used by. The Accounts Receivable business function depends on the Acrobat application item, and the Acrobat application is used by Accounts Receivable. Similarly, your business function may depend on other dependency groups like software technology or hardware to accomplish a business process.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon ( ).
3. Click the link to the record in the **Name** column in the **In Draft** state.
4. To review a group and identify the items within each group, click the **Dependency Assessment** tab.
5. To add an item to a dependency group, click the **Add New** button of that container.
6. To filter items from all the records, click the **From all records** button.
   a. Click **Next**.
   b. Select items from the Add items pop-up.
   c. Click **Add**.
7. To filter an item based on its relationship with the dependency group, click **Based on CMDB dependencies (Level 1)**.
   a. Click **Next**.
   b. Select items based on the relationship.
   c. Click **Next**.
   d. Select the item.
   e. Click **Add**.
   The dependency group grid lists items that depend on the BIA. If you add an item from all the records, then the **Relationship source** is **BCM**. If it is based on CMDB dependencies, then it is **CMDB**.

   **Note:** If you select an item **Based on CMDB dependencies (Level 1)**, only those items that are directly related or in the level 1 of dependency based on the relationship types identified in CMDB are listed in the Add items pop-up. On the other hand, if you select **From all records**, then all items from the respective table, irrespective of its relationship in CMDB, are displayed and are tracked up to a maximum of five levels.

8. To view the details of the dependent item, click ⓘ.
   The dependency details of the item that your business function depends on opens in a new tab. You can update the required recovery timeframe, required data backup, and the description of its use in the business function, and save the details.

#### View business impact analysis details

Use the **Details** tab to view the general information of the business impact analysis. You can also adjust the recovery time objective and recovery point objective results of the primary element as per your requirement.

### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon (  ).
3. Click the link to the record in the **Name** column in the **In Draft** state.
4. To view the details of the business impact analysis, click the **Details** tab.

General Information

View the general details of an assessment for the Business Impact Analysis such as the name of the BIA, its description, and the business unit and department that it pertains to. You can also view the template that you have used to create the BIA.

Results

You can track the results at the asset level. Hence, the primary scope is to recover the primary element or the asset. Defining recovery requirements depends on the type of disaster and the time by which each asset must be recovered.

- **Recovery tier**: The level of criticality at which the primary element is in terms of its recovery.
- **Recovery time objective** (RTO): The maximum time by which the business should recover the primary element or asset after the business disruption.
- **Adjusted RTO**: If you want to adjust the calculated RTO, then edit this field to add your value.
- **Reason for adjusted RTO**: Enter the reason for adjusting the RTO value.
- **Recovery point objective** (RPO): Point in time at which the primary element must be restored following a disaster. It also indicates the maximum amount of data loss that a business can sustain during a disruptive event.
- **Adjusted RPO**: Edit this field to enter your RPO for the primary element.

  **Note:** **Recovery point objective** and **Adjusted RPO** fields appear only if the primary element requires data backup and is flagged as **Yes** in the Element Definition form.

- **Reason for adjusted RPO**: This field appears when you enter a value in the **Adjusted RPO** field. Enter the reason for adjusting the RPO value.
- **Confidentiality**, **Integrity**, and **Availability**: If the primary element includes critical data, then add Confidentiality, Integrity, and Availability (CIA) details. CIA details are basic security goals that the BIA must be compliant with. Non-compliance to these standards may lead not only to huge business and productivity loss but also credibility loss.

  **Note:** The **Confidentiality**, **Integrity**, and **Availability** fields appear only if you have already set the **Include CIA** field as **Yes** in the  that you have used.

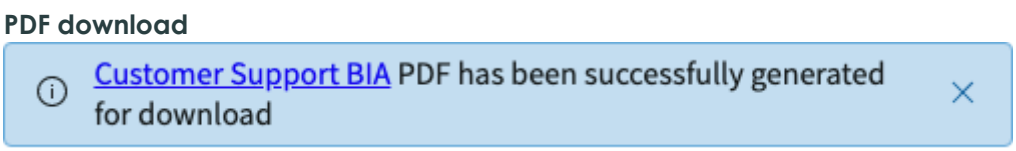
  If you have not adjusted the RTO and RPO values, you can still view the system-calculated RTO and RPO values in their respective fields.

Activity

Additional comments about the BIA.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Save**.
6. Click the **Generate PDF** button to generate the BIA in a PDF format.
   A message appears that the PDF has been generated.




   Click the link in the message to download the PDF.

   - If you have view-only access to the BIA, the option to generate a PDF helps you to download the document to your local hard drive.
   - You can download the BIA before its **Approval** state.
   - By default, the PDF is generated and attached after the BIA is approved.

7. To move a BIA from **Approved** to **Draft** state, click the **Edit** button.
8. To create a copy of the BIA, click **Copy** button.
   If you have the permission to read and create a BIA, then you can also copy the BIA.

   a. Enter the name of the new BIA in the Copy impact analysis pop-up.
      The copy action creates an exact replica of the BIA with the name that you enter in the Copy impact analysis pop-up. It also copies all its dependencies and dependency groups on to the new BIA.

   b. Click **Confirm**.

      - The new BIA that is copied from the original BIA has all the RTO, RPO impact, dependency assessment structural details similar to the original BIA.
      - However, the impact category details for each of these assessments are editable for you to assess the dependency details exclusively for the copied BIA.
      - If the impact categories of the RTO and RPO impact assessments in the original BIA are in the **Complete** state, then the impact categories in the copied BIA are in the **Complete** state.
      - Therefore, you must assess and enter the disruption duration, response, and required recovery timeframe relevant to the copied BIA.
      - You can assess the details in the **Results** section. The RTO and RPO values are recalculated after you complete the assessments.
      - Activities and Work notes are not copied to the new BIA. Enter this information relevant to the new BIA.
      - Any attachments attached to the original BIA in any format are copied to the new BIA. However, the PDF generated for the original BIA using the **Generate PDF** button will not be copied over to the new BIA as the assessment data pertain to the original BIA. Since you have the flexibility to modify the assessment details in the copied BIA and generate a PDF, copying the PDF generated for the original BIA has no relevance.

      **Note:** You can delete a BIA and its related tables in the **Draft** state. The BCM planner and program manager can delete a BIA that is in the **In Review** and **Returned** states whereas, a BCM admin can delete a BIA irrespective of its state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### View approval state flows for a business impact analysis

View the approval state transitions sent at each level of the approval process, and the details of the approvers as you direct the business impact analysis through multiple levels of approvals.

## Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager, sn_bcm.viewer

## Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon (  ).
   You can view approval records for a business impact analysis (BIA) that is any state except **Draft** and **In Review** states.
3. Click the link to the business impact analysis record in the **Name** column.
4. To view the approval details of the BIA, click the Approvals related list.
   If there are no approval records in the requested state for the BIA, then you can either **Reject** or **Approve** the BIA.

   **Note:** If you are a BCM Program Manager, then you can see the **Approve** and **Reject** buttons.

5. Click the link to the approval record in the **Name** column.
   You can view the name of the approval, approval level, its current state, and the details of approvers such as users and groups.
6. To view the approval history of the impact analysis, click the **Details** tab.

   a. Click the Approval History related item.
   You can view the complete approval history of the approvers and the details as to when it was created.

   State transitions for multiple levels of BIA approvals:

   Not Yet Requested

   State where an approval is not yet sent to the approvers at a respective level.

   Requested

   Approvals are sent to the approvers of that level. Correspondingly, the state of all successive levels of approvals turns to Not Yet Requested.

   Approved

   One or more approvers have approved the BIA at the respective level. Correspondingly, the state of the succeeding level of approval moves to Requested.

   Rejected

   One or more approvers have rejected the BIA at a particular level. Even if one approver rejects the BIA, then it moves to **Rejected** state. Correspondingly, the state of all succeeding levels of approvals moves to No Longer Required.

   No Longer Required

   If the approvers at a level have approved or rejected the BIA, then the state moves to No Longer Required for all succeeding levels of approvals.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Update dependency details of a BIA in Self Service as a contributor

Use contributor role to update the disruption duration of the impact category result, RPO Impact analysis responses, state of the impact dependency group, and the work notes in the Activity related item.

#### Before you begin

Role required: sn_bcm.contributor

If you are a BCM contributor and is part of the Contributors list, then you can update the dependency details of a business impact analysis (BIA).

#### Procedure

1. Navigate to **All** > **Self-Service** > **My Impact Analysis**.
2. View the list of business impact analysis assigned to you and the BIAs that you can contribute to.
3. Click a impact analysis record.
4. Click the Impact Category Results related list.
5. Select any RTO impact assessment record to update its disruption duration details.
6. To update the impact analysis response, click the RPO impact category record.
7. To update the state of the impact dependency group, click the Impact Dependency Group related list.
   You can also add, update, and delete dependencies under the dependency group.
8. To add work notes to the BIA, click the **Activity** tab.
9. Click **Update** after your changes.

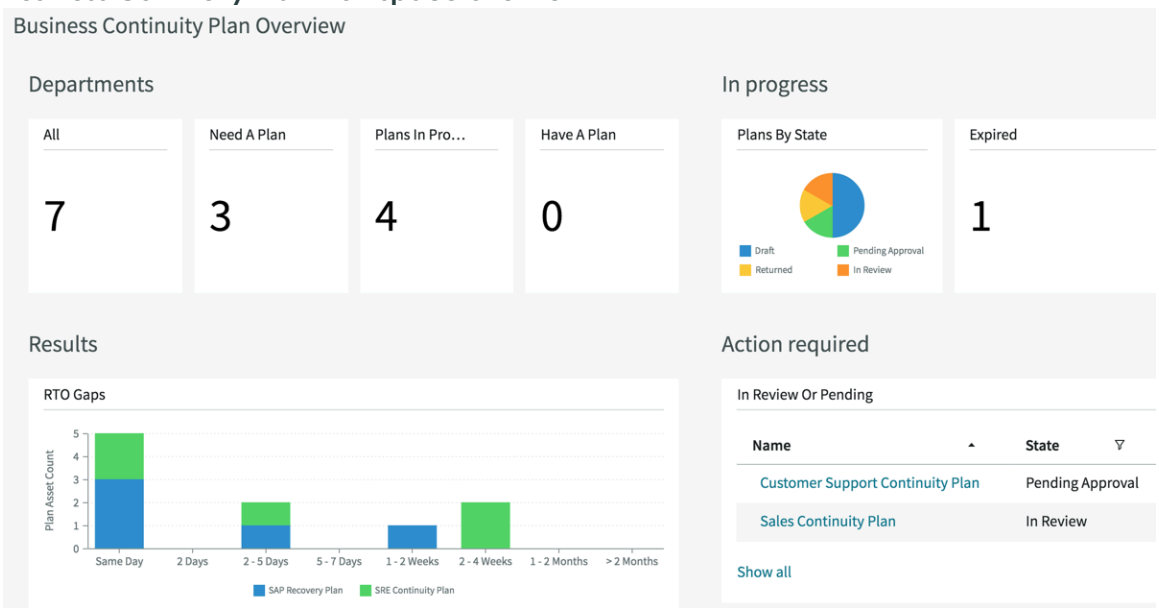
## Structured workflows for Business Continuity Planning

Business Continuity Planning (BCP) helps you enact and mitigate risk at the time of an event by addressing action items such as plan assets, activities, recovery teams, documentation, policies, and procedures.

BCP consolidates all the data needed for managing business continuity and disaster recovery plans in Now Platform®. It organizes a catalog of enterprise data into a single system of records. Instead of creating records, you can simply select the required data. Creating plans then becomes simple and effortless by taking advantage of the existing information and arranging it in a logical association of data for recovery.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

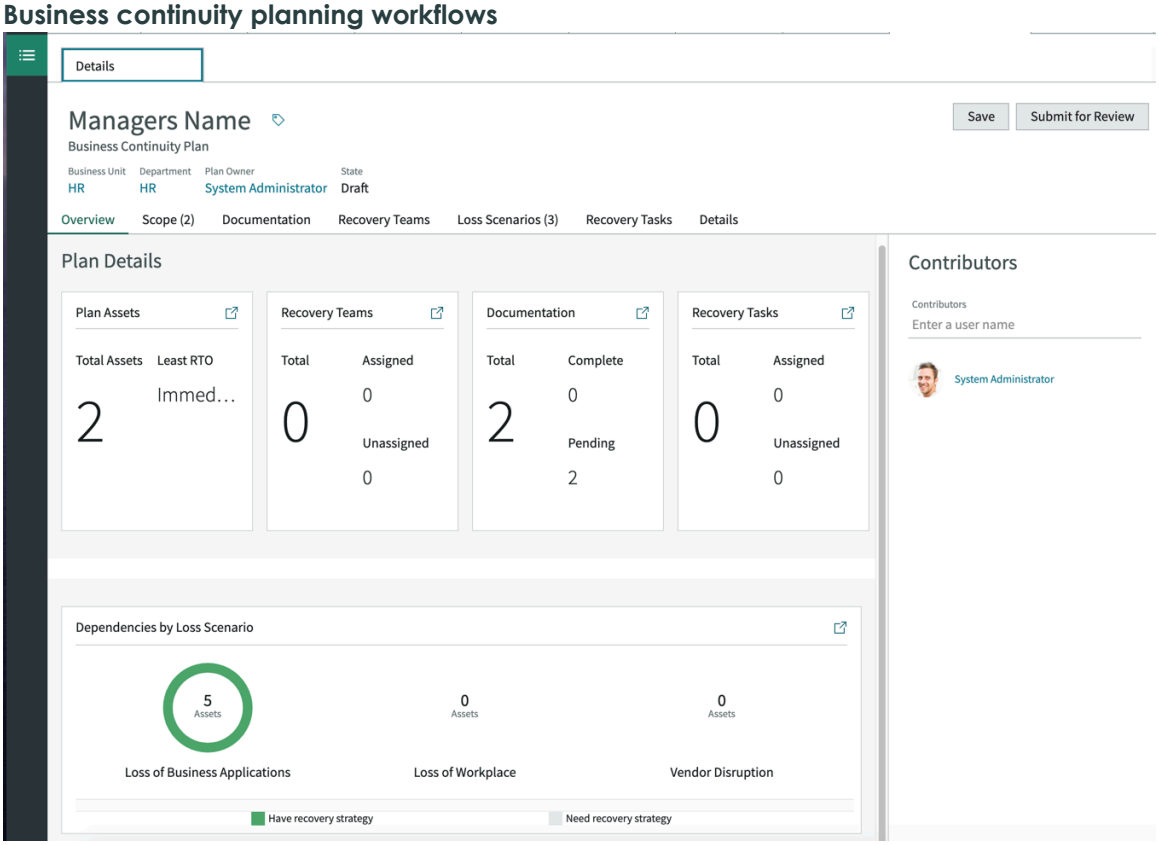
### Business Continuity Plan workspace overview




The program manager, planner, and viewer get a custom workspace to work on, which presents them with the current status of plan-related activities. The workspace is a secure portal to open the plans that are available for access to the user with a particular role.

You can build your plan within a single user interface with the ability to open a plan tab to complete a task. You can move on to the next plan task to add, delete, or update the details of the plan.

### Business continuity planning workflows




With comprehensive action plans in place for different possible disruptive scenarios, and a dedicated team with responsibility to act quickly at the time of a loss scenario, your organization is equipped to face a crisis or any adverse situation.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create a business continuity plan from a plan template

As a program manager you can create a plan for the respective business units that can be used in times of business disruption. You can use a specific plan template for each plan type to streamline the process of a plan creation.

## Before you begin

Role required: sn_bcm.program_manager, sn_bcm.planner

## About this task

You can create a plan using a pre-configured plan template that suits your requirement. Using the plan template gives you a standard plan layout automatically adding document sections, loss scenarios, and identifying primary elements that are to be recovered. Plan templates help you to focus on the plan content, its tasks, and the effective implementation of the plan.

Creating a plan helps an organization to identify processes, locations, and assets that must be recovered as a priority when there is a disruption. Selecting a plan type helps to identify the elements for recovery and the time by which it should be done.

As a BCM program manager you can create a plan by clicking the **New** button. When you select a template for the plan, all the related information in the template is copied over to the plan after you submit.

## Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. To create a plan from the Business Continuity Home page, click **Create a Plan**.
3. To view the list of existing plans in different states and to create a plan record, click the lists icon ( ).
   a. Click **In Draft** state in the Planning list.
   b. Click **New**.
4. Enter plan details in the Create Plan modal form.
5. Enter a name for the plan and select a plan template.

   Describe the plan name within 255 characters following a naming convention exclusively for your business teams.

   The details of the referenced template are copied over to the plan. Select the business unit, department, and the plan owner applicable to the plan.

6. Click **Submit**.

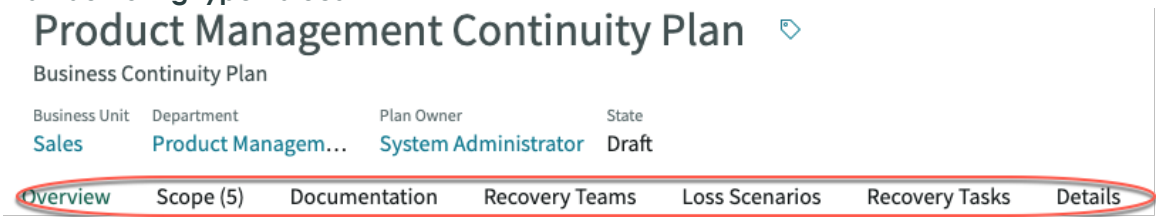
   The plan that you created opens up in the record view. This view displays the details of the plan under the headers **Business Unit**, **Department**, **Plan Owner**, and **State**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:**

The tabs that are available in the Plan view depends on the value that you have selected in the **Plan authoring type** field of the Plan Template that is used in this plan.

**Plan authoring type values**




When you create a plan using a template, the plan documentations associated to the plan template are copied over to the documentation section of the plan that you created.

7. Review the plan details in the **Overview** tab.
8. Click the **Details** tab to update the plan details.
9. To save the plan and update its details later, click **Save**.
10. To save and submit it for review, click **Submit for Review**.

**Note:** You can submit the plan for review only when it is **In Draft** stage.

When you submit the plan for review, the plan moves to **In Review** state.

As a plan owner, you can add details to the plan and move it across different states to get it approved finally.

**Note:** The **State** field is read only. It indicates the status of the plan. Hence, your action on the plan in the UI takes it through to its approved state.

In Draft

It is the state when your plan is under edit. Add documentation sections to the plan, identify recovery teams and set up recovery tasks for the owners, and submit the plan for review.

To submit for review, ensure that a BCM Lead is assigned to the plan. Otherwise, you can submit the plan for approval.

After the plan owner submits the plan for review, the state changes to **In Review**. The state of the plan changes to **Submit for Approval** for the plan owner.

In Review

The plan owner can review, edit, and submit the plan for approval.

Pending Approval

When you click **Submit for Approval**, the plan is set to **Pending Approval** state. The approval configurations, approval levels, and approval rules are evaluated against the plan to determine the approvers. If there are no approval records in the requested state for the plan, then as a BCM program manager you can either **Reject** or **Approve** the plan. The state of the plan and its related tables is read only.

Returned

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the plan is rejected, the state is set to **Returned** state.

Approved

When the plan is approved, it moves to **Approved** state.

The plan and all its related tabs are read only. Your only option to change the status at this state is to move it to **Archived** state.

Archived

When you archive the plan, it becomes read only. All underlying tables from where the plan retrieves its data to populate in the plan assets, related asset dependencies, recovery strategy, documentation, recovery teams, loss scenarios, and recovery tasks tabs become read only. You cannot edit the information in these tabs anymore.

**Note:** A scheduled job runs weekly to move the plans that have expired to **Archived** state.

11. To export the plan to different locations and make it available for people to execute the plan in a crisis situation, click **Generate PDF**.

**Note:** You can generate a PDF if you are a plan contributor (sn_bcp.plan_contributor) or plan manager (sn_bcp.plan_manager).

You can generate a PDF of the plan in all states except **Approved** and **Archived** states. If the plan is approved, then by default a PDF is generated and attached to the plan.

The plan is exported in its entirety with its summary, recovery teams, loss scenarios, recovery tasks, and an appendix table listing the contact number of every member who is part of the recovery team.

### View plan details in scorecards

Use the **Overview** tab to gain a quick understanding of how robust your business continuity and emergency plans are. This tab gives an overview of the scores of important plan elements, each as a scorecard.

#### Before you begin

Role required: sn_bcm.program_manager, sn_bcm.planner

#### About this task

Your emergency action plan must be customized to your workplace and include information about all potential sources of emergencies. The plan must be comprehensive with details of:

- the assets that have to be recovered
- the teams that are responsible for the recovery of each type of asset
- a designated group to which the plan is assigned
- an owner identified to the assignment group
- documentation detailing how the plan must be executed

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon ( ).

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

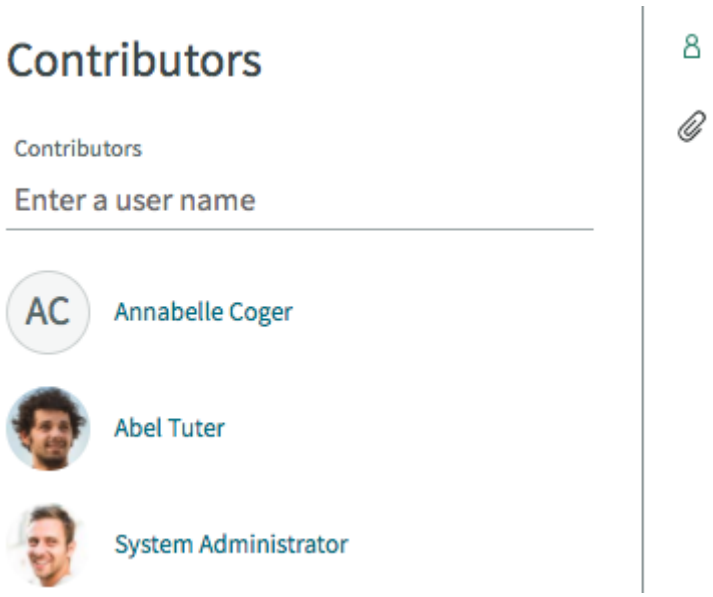
3. Click **In Draft** state in the Planning list.
4. Click the link to the plan record in the **Name** column.
   In the **Overview** tab, you can see the scorecards that are graphical representations of the progress of the plan for making it complete towards its goal.

   The different scorecards that are available to view in the **Overview** tab depends on the value that has been selected in the **Plan authoring type** field of the Plan Template used in this plan.

   **Note:** If your plan is in **Approved** state, then you can view the **Plan Usage and Results** section. However, you can view all the details of a plan in the **Plan Details** section irrespective of the plan being in any state. For more information, see Plan overview scorecards for plan usage details.

5. To complete the documentation sections that are in **Pending** state, identify teams and individuals for the unassigned recovery teams, or assign groups to carry out specific plan activities, click go to section icon ( ) in the respective scorecard widget to add the required information and set the plan to complete.
6. To add contributors to the plan, click the **Contributors** field to select the users.

**Contributors card in the Overview tab**




   To make a business continuity plan complete and robust, you need inputs from people who can assist and contribute information on the plan. These contributors can also be users to whom you can assign specific tasks. You can add as many contributors as the plan requires.

7. To remove a contributor from the plan if no longer required, click the **Remove** button next to the name of the contributor.

### Plan overview scorecards for plan usage details

The **Overview** tab gives you the details of the plan and the exercise and actual events that use the plan. It also indicates how successful the plan was in recovering the assets in a loss scenario.

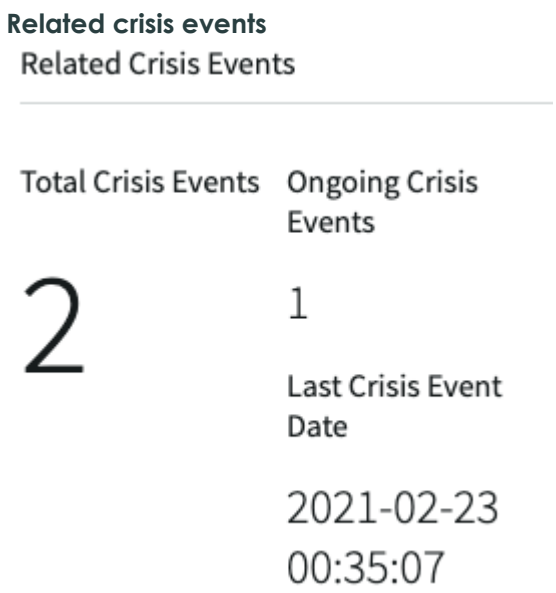
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Plan usage and results

The Plan Usage and Results section shows the details of the crisis and exercise events that use the current plan that you are viewing.

Related Crisis Events

- Total Crisis Events: The total number of crisis events that use the current plan.
- Ongoing Crisis Events: The number of crisis events that are currently in progress.
- Last Crisis Event Date: The actual end date and time of the last crisis event that happened.

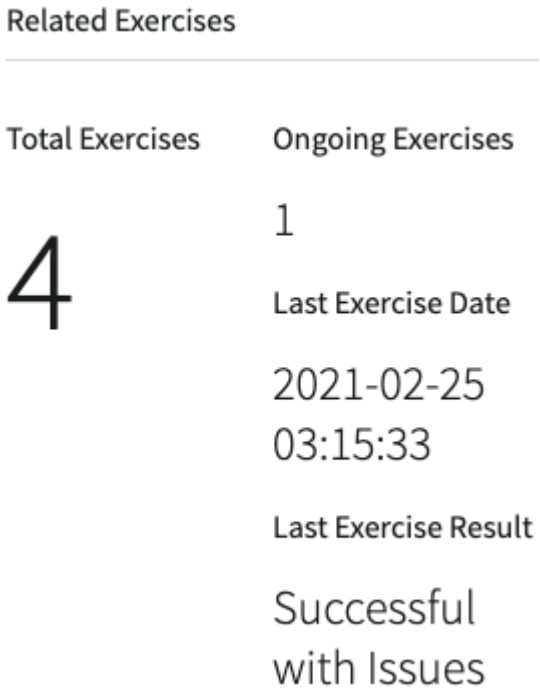



Related Exercises

- Total Exercises: The total number of exercises that use the current plan.
- Ongoing Exercises: The number of exercise events that are currently in progress.
- Last Exercise Date: The actual end date and time of the last completed exercise event.
- Last Exercise Result: Indicates whether the last completed exercise event was successful or not.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related exercises**




Exercise Results

The color-coded donut indicates the number of completed exercise events that were successful, unsuccessful, and successful with issues.

**Exercise results**



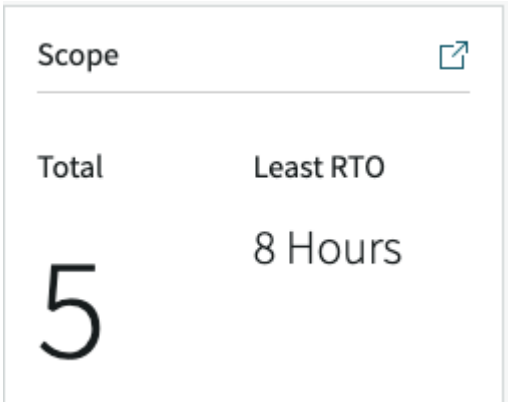

## Plan details

Scope

Displays all the assets identified in the plan as **Total**. Out of all the RPO and RTO that a primary element supports, the minimum value of RPO and RTO is displayed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Plan assets scorecard**




Recovery Teams

The scorecard helps you to identify teams and individuals with clear guidelines of responsibilities to act at the time of a crisis.

The assigned score indicates that a recovery role of a plan has been assigned to a group or a user. The unassigned score indicates that the recovery role is not assigned to any group or user.

**Recovery teams scorecard**

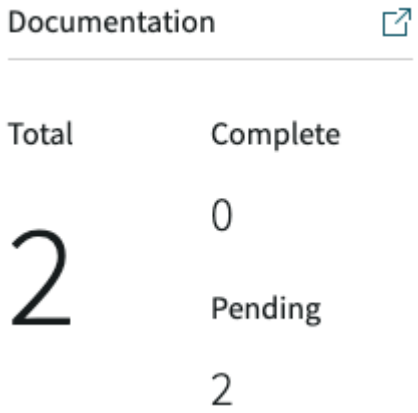



Documentation

Displays the total number of documentation sections that are attached to the plan. The breakdown shows the status of the documentation sections that are updated according to the plan and in **Complete** state. The **Pending** state indicates the documentation sections that are still under edit.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

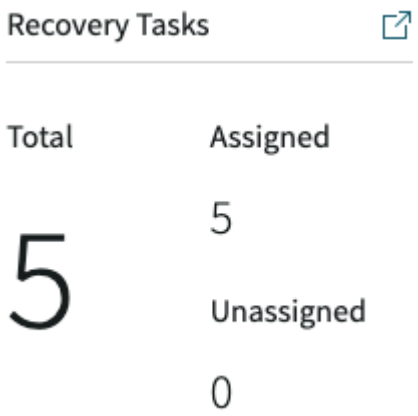
**Documentation scorecard**




Recovery Tasks

The recovery tasks scorecard indicates a group and an owner for the group, identified to carry out the activities of the plan during the recovery process.

**Recovery Tasks scorecard**



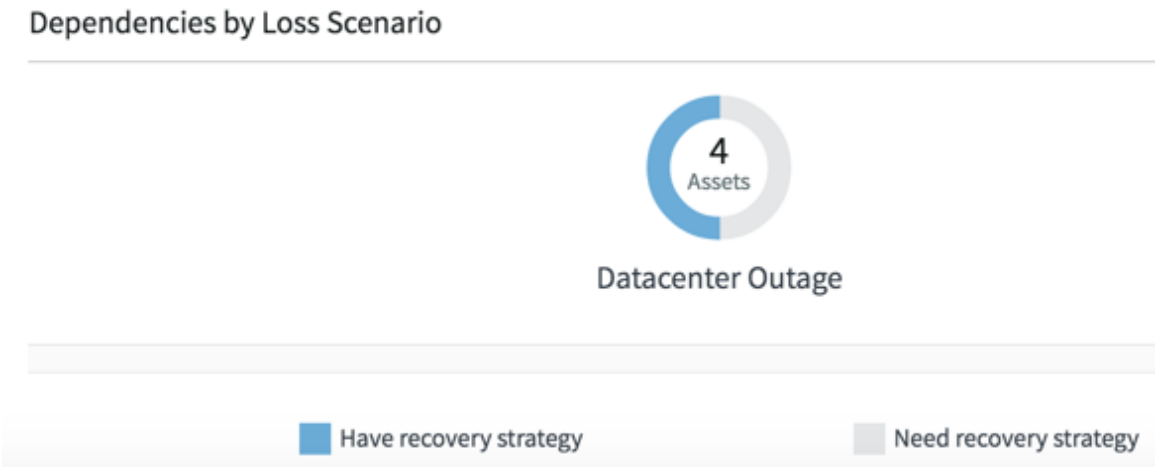

Out of the total number of activities identified for the plan, the assigned score indicates the number of activities for which groups have been assigned. Unassigned score indicates plan activities for which groups have not been assigned.

Dependencies by Loss scenario

The donut chart shows the assets covered by a strategy, and uses colors to indicate whether the asset has a strategy or not. A loss scenario plan must have at least one strategy for an asset. However, you can also have a single strategy covering multiple assets.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Dependencies by loss scenarios




### Add an asset to the scope of a business continuity plan

Use the **Scope** tab to add an asset to the scope of the plan. If the business impact analysis (BIA) application is installed, you can view the primary elements defined in the plan template, its recovery time objective (RTO) and recovery point objective (RPO) details, and the business impact analysis.

#### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon ( ).
3. Click **In Draft** state in the Planning list.
4. Click the link to the plan record in the **Name** column.
5. Click the **Scope** tab.
   If the plan is created from a plan template, you can view the primary elements defined in the plan template.
6. To add new scope to the plan, click **Add**.
7. On the Add Items modal, select the plan asset.
8. Click **Add**.
   Assets that are displayed in the Add Items modal belong to the element definition type identified in the **Primary element recovered** field of the plan template.

   If an asset has an approved BIA attached to it while adding the plan asset, then the approved BIA is automatically added in the **BIA** column of the asset.

   If the BIA is attached to the plan scope, then you cannot edit the RTO and RPO as they are values populated from the BIA.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:**

- If the BIA application is installed, then **RTO** and **RPO** fields are visible and non-editable. **BIA** field is visible and editable. You can attach a BIA by clicking the link BIA icon ( ).
- If BIA is not installed, then **RTO** and **RPO** fields are visible and editable.
- If an approved BIA is attached to the plan, then **RTO**, **RPO**, and **BIA** fields are populated with values and they are read only and non-editable.

9. To update a plan asset or to link a BIA to it, click the asset in the **Name** column.

   a. Click the link BIA icon ( ).
   If there is an approved BIA for the asset, then the BIA is automatically attached to the asset when you click the link. If you have adjusted the RTO and RPO values based on the criticality of an asset, then the Adjusted RTO and Adjusted RPO values take precedence over the system-calculated RTO and RPO values. The adjusted RTO and RPO values are displayed in the **Recovery Time Objective** and **Recovery Point Objective** fields when you click .

   b. Click **Save**.

10. To remove an asset from the plan list, select the item and click **Remove**.

### Add related assets and related plans

Identify related assets and their referred plans to recover the assets in your planning stage. Reuse the configuration item relationship data that flow from CMDB to business impact analysis (BIA) during dependency assessment to identify the assets in your plan.

#### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

#### About this task

With this feature enhancement, the relationship data of the configuration items in CMDB flow in to the business impact analysis (BIA) when you Add dependencies based on CI relationships in CMDB. If you have done the BIA, then the related assets data flow to the planning phase. In the planning phase, you can identify these BIA-dependent items as related assets. Additionally, if you have done the BIA and if your related assets has a plan, then you also have the capability to add the plan existing for the related assets as related plans in the planning phase, and as sub-plans in the execution phase of the event recovery process.

Therefore, instead of identifying new assets and creating plans to recover the assets you can use the BIA-dependent items that are added as configuration items from CMDB based on their CI relationship and reuse these items as related assets in the planning stage.

This feature gives you the ability to:

- Identify the related assets based on dependencies established in the CMDB and BIA during planning.
- Create a main plan and set a task that refers to another related plan.

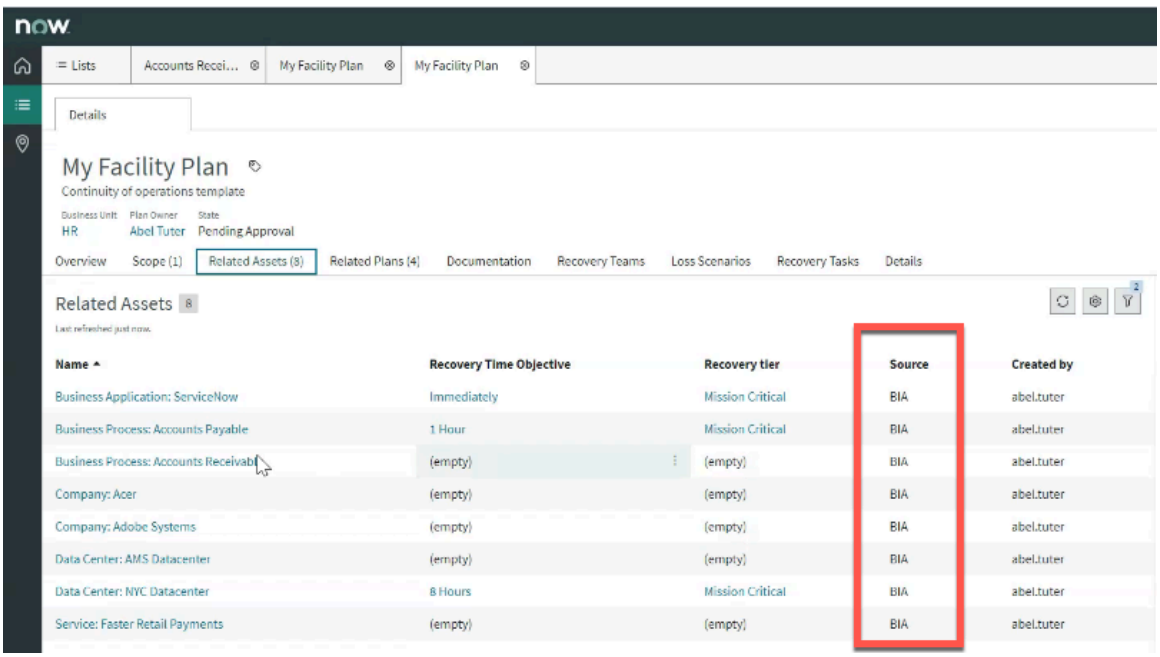
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon ( ).
3. Click **In Draft** state in the Planning list.
4. Click the link to the plan record in the **Name** column.
5. Click the **Related Assets** tab to view the assets that are pulled from the BIA to the plan. If you have added a business process or a location as an item in the **Scope** tab, and if the scoped item is related to the BIA, then all the related assets of the BIA are lined in to the **Related Assets** tab of the plan. In other words, the CMDB configuration item added as a dependency in BIA is pulled into the plan as related assets. The source of these related assets is displayed as BIA.

   When you create a plan, you also select a primary element that the plan covers. Based on the scope that you selected in the business continuity plan or the primary element of the plan, the application adds the related assets and related plans during the planning phase. These items could be business processes, critical business applications, data centers, or resources working from a location. All these dependencies if stored in the BIA are copied over to the plan in the **Related Assets** tab in addition to other dependencies that are added while creating the BIA.

   **Related assets tab**




> **Note:** Unless you do the business impact analysis, the related items of the configured item data will not flow to the plan, although you have the option to manually add the related assets and related plans in the planning phase.

6. To add an asset manually, click the **Add** button.

   a. Select a type of the impacted item in the Add Items pop-up.

   b. Click **Next** and select the items that belong to the impacted item type.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Click **Add**.

> **Note:** If the item did not come from the BIA but added during the planning phase, then the source of the impacted item that you added is **Manual**.

7. To remove a related asset, select the related asset and click **Remove**.
8. Click the **Related Plans** tab to view the plans that are related to the items in the **Related Assets** tab.
   After the assets are copied over to the plan, if there are plans attached to any of the related assets, then these plans are automatically pulled and listed in the **Related Plans** tab. Assets in the plan are those that are to be recovered by the plan during the event.

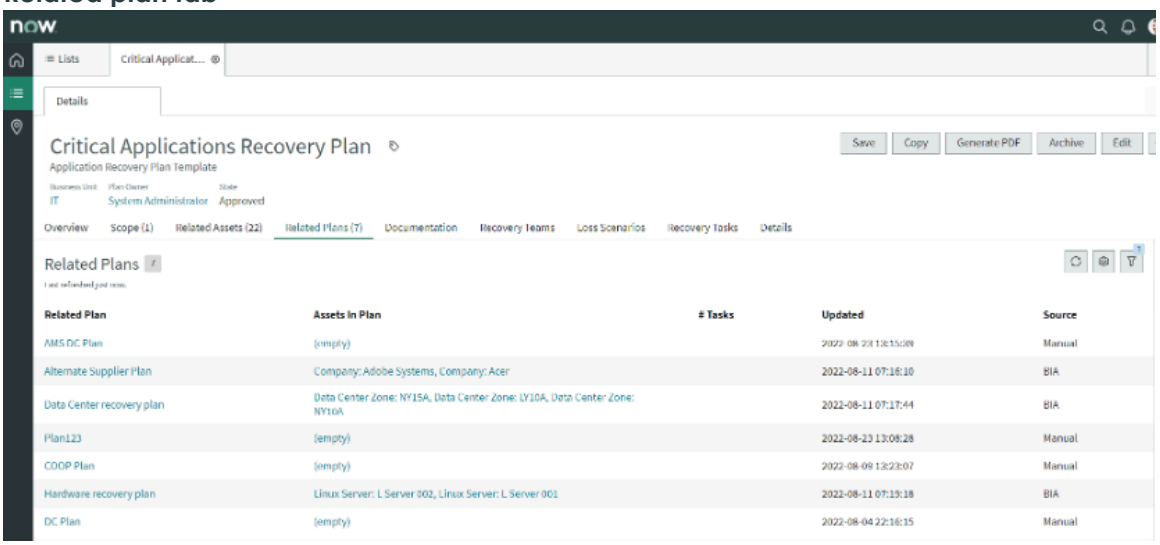
   When the related plans are pulled into the planning phase, you can also create the recovery tasks. As a planner you can set a sequence to the execution of the recovery tasks of the main plan and its dependent sub-plans.

   If you have not done the BIA or scoped the plan to a BIA, you can manually add plans at this stage.
9. To add a plan manually, click the **Add** button.

   a. Select a plan in the Add pop-up.

   b. Click **Add**.

**Related plan tab**




> **Note:** The source of the related plan that you added is **Manual**, as the plan did not come from the BIA but added during the planning phase.

10. To remove a related plan, select the related plan and click **Remove**.

### What to do next

You can refer one of the related plans in a recovery task of the main plan and sequence the order of execution in the event.

### Create and manage plan documentation sections

Use the documentation section to document the recovery capabilities of the plan.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

### About this task
Document all additional information such as the goals, objectives, and scope that are required in the context of your plan as separate sections within the document.

### Procedure
1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon ( ).
3. Click **In Draft** state in the Planning list.
4. Click the link to the plan record in the **Name** column.
5. Click the **Documentation** related list of the plan.
   You can view each section of the documentation in a separate text box. The documentation sections that are part of the plan template, which you used to create the plan, default to this plan. You can create new sections to the documentation and edit existing sections as well.
6. To edit a documentation section, click the edit icon ( ).
   Use this icon to edit the title as well as the text in the description of the documentation section.
7. To edit the text in a section, click the **Edit** button in the text box.
8. To undo all your updates and revert to the original text of the documentation section, click **Reset to template** and click **Reset** to confirm your action.

   **Note:** **Reset to template** button is enabled only when the document section is in Pending state and not in Complete state.

   When you reset, both the title and description along with the text in the documentation section are reset to the title, description, and documentation content in the plan template.

9. To delete a documentation section, click the delete icon ( ).
   This action deletes the documentation section.
10. To create a section in the documentation tab, click **New section**.
    a. In the New section pop-up, enter a title and a description for the section.
    b. Click **Create**.
    c. Click the **Edit** button to enter the contents in the text box for the section.
11. To save the updates and continue to edit the content, click **Save**.
12. To save and exit the edit mode, click **Complete**.
    After you click **Complete**, both the and icons are disabled. To enable the icons, click the **Edit** button in the documentation section text box.
13. To view the subsequent section and scroll through all the sections, collapse the section after you complete editing.

    Change section order at the plan level

    You can change the order in which the sections appear in the **Documentation** related list to help the user review the sections in a logical sequence. However, you must set the order preference for the sections by entering an integer value

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

in the **Order** field of the Plan Documentation form for each documentation section in the plan. This customization overrides the order preference set at the plan template level.

Change section order at the plan template level

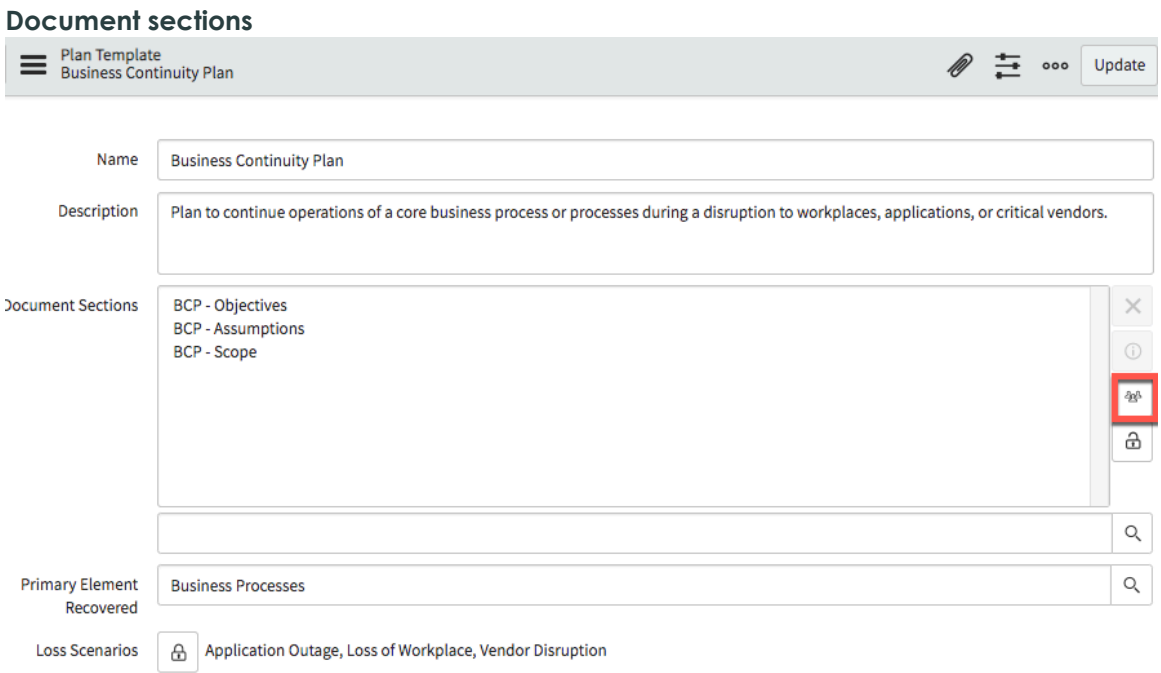
You can define the order of document sections in the Plan template as well. This order is applied to all the plans that use the template. However, only a BCM administrator can change the order of the sections in the Plan Template form, when the template is created.

**a.** To rearrange the section order, navigate to **Business Continuity** > **Plan Configuration** > **Plan Templates**

**b.** Click the plan template in the **Name** link.

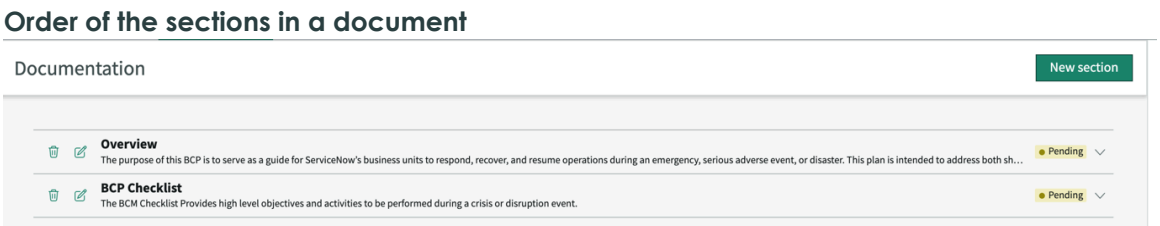
**c.** Click unlock document sections icon ( )

**d.** Click the add/remove multiple icon ( ) and move the items in a preferred order in the **Document Sections** field.




**e.** Click **Update**.

As a program manager, planner, viewer, or BCM administrator, you can only view the rearranged order of the sections in the workspace when your plan uses that template.




## Assign roles and responsibilities to recovery teams

Identify individuals and groups and assign them to the recovery team so that they are aware of their roles and the responsibilities of the role to act in a crisis situation.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

### About this task
Business continuity planning workspace guides you step by step to complete your plan by creating a recovery team, defining roles and responsibilities for users, assigning the users and groups appropriately to the recovery team, and directing the team to execute the plan.

### Procedure
1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon (  ).
3. Click **In Draft** state in the Planning list.
4. Click the link to the plan record in the **Name** column.
5. Click the **Recovery Teams** tab of the plan.
6. To create a recovery team and assign users and groups to the team, click **New**.
   You can create a recovery team by entering a name and description or update an existing one. Select one or more users and groups from the respective lists. The description for the recovery team also indicates the responsibilities of the users and groups who are assigned to the recovery team. You can also create a recovery team and leave the user and group assignment for later.
7. Click **Submit**.

#### Identify loss scenarios and align them to a business continuity plan

When you create a continuity plan or a recovery plan for a department or a business unit, it is necessary to identify and align loss scenarios to the plan.

### Before you begin
Role required: sn_bcm.program_manager

### About this task
As a plan owner identification of loss scenarios helps you to be prepared for any sudden disruptive event and continue with business functions as usual.

When you create a plan using a plan template, the loss scenarios that are identified in the plan template automatically get associated to the plan that you created. Your plan has a basic set of loss scenarios attached to it. You can then add additional loss scenarios to the plan as per your requirement.

### Procedure
1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon (  ).
3. Click **In Draft** state in the Planning list.
4. Click the link to the plan record in the **Name** column.
5. Click the **Loss Scenarios** tab of the plan that opens.
   Use this tab to plan for every disruptive scenario that you can predict, and to manage response and recovery in such a situation.
6. Click **Add** to add additional loss scenarios to the plan.
7. Select the scenario names from the Add Loss Scenarios modal form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Click **Add**.

   The loss scenario is associated to the plan. The Plan Loss Scenario table [sn_bcp_plan_loss_scenario] stores the relationship between the plan and the loss scenario.

9. To add related asset dependencies to the loss scenario of the plan, click the link to the loss scenario record in the **Name** column.
10. Click **Add** in the Related Asset Dependencies related list to add dependent items.

    a. To filter items from all the records of the underlying element definition, click the **From all records** button.
    If the loss scenario is loss of business applications, then all impacted applications are filtered and listed.

    b. Click **Next**.

    c. Select items from the Add items pop-up.

    d. Click **Add**.

    a. To filter items that depend on the plan scope, which is attached to the BIA, click **Based on plan scope**.
    b. Select the plan scope from the list.
    c. Click **Next**.
    d. Select the dependencies of the selected plan scope item attached to the BIA.
    e. Click **Add**.

### Establish recovery strategies for critical asset dependencies

Use the **Loss Scenarios** tab to add asset dependencies and identify recovery strategies to deal with various loss scenarios. A plan, complete with recovery strategies for the identified loss scenarios, helps to address gaps that exist.

## Before you begin

Role required: sn_bcm.program_manager or sn_bcm.planner

## About this task

As a program manager, you can check if there are recovery strategies for various loss scenarios of the plans owned by the planners. Such assessments enable you to be prepared for those scenarios.

When you see the details of a loss scenario associated to a plan, you can also view the assets that are attached to the plan, and the recovery strategies for each of these assets. For example, NYC datacenter can be a related asset for a datacenter outage loss scenario of a customer support plan. You can create a recovery strategy by estimating the time to implement the strategy to get the NYC datacenter up and running.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon ( ).
3. Click the **In Draft** state in the Planning list.
4. Click the link to the plan record in the **Name** column.
5. Click the **Loss Scenarios** tab of the plan.
6. Click the link to the loss scenario record in the **Name** column.
7. To add a related asset to the existing list of assets that can be impacted and dependent on the plan loss scenario, click the **Related Asset Dependencies** tab.
   For more information, see Identify loss scenarios and align them to a business continuity plan.
8. To remove an asset from the plan, select the item and click **Remove**.

   **Note:** You can add or remove an asset, dependent on the plan, only if you are a program manager or owner of the plan.

9. To establish a strategy and recover a critical asset, click the **Recovery Strategies** tab.
   a. Click the **New** button.
   b. Enter a name and description for the recovery strategy and determine the implementation details to recover the asset.
   c. Click **Save**.
10. To add a recovery task to the recovery strategy of a plan's loss scenario, click the **Recovery Tasks** tab.

    You can create a recovery task at the recovery strategy level and also at the plan level.
    See: Create, update, and group recovery tasks.

### Create, update, and group recovery tasks

Create tasks in a plan to recover your business from various disaster situations. Prioritize the tasks by determining the critical assets that have to be recovered and estimate the time by which the task must be completed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

### About this task
Assign the task to a group, identifying an owner, to execute the processes and procedures of a recovery. The task has details of the item to be recovered and the time by which it should be accomplished.

### Procedure
1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon (  ).
3. Click **In Draft** state in the Planning list.
4. Click the link to the plan record in the **Name** column.
5. Click the **Recovery Tasks** tab of the plan.
   The **Recovery Tasks** tab displays all the data in editable lists. You can prioritize the tasks by sorting, grouping, and filtering each column of data the way you want.
6. To create a recovery task, click **New**.

   a. On the form, fill in the fields.

**Create Recovery Task form**

| Field | Description |
|---|---|
| Task ID | Number assigned to each task. Indicates the position of the task with respect to other tasks in the grid.<br><br>Enables you to view the tasks in a particular sequence especially in a printed PDF. |
| Scope | Asset that the task recovers. If field is empty, the task recovers asset at the plan level. Otherwise, it recovers the recovery task scope. |
| Recovery team | Team to which the recovery task is assigned. |
| Assignment group | Group to which the task is assigned. |
| Refer a different plan | Option to indicate that the recovery task is not an individual task, but refers to a separate plan with its own set of tasks.<br><br>If the check box is clear then the recovery task is executed normally as per the task ID sequence at the time of exercise. |
| Select plan | Plan from the list in the **Related Plans** tab. If the task has a referred related plan within, then the tasks of the referred plan are executed before the execution continues |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | sequentially with the rest of the recovery tasks in the main plan.<br><br>Field appears only if the **Refer a different plan** check box is enabled. |
| Assignment group | Group to which the task is assigned. |
| Dependencies | Tasks dependent on the asset and plan, ruling out cyclic dependency. |
| Documentation | Details about the execution of the plan. |
| Recovery strategy | Objective to recover an asset identified in a plan. |
| Completion deadline | Time by which the recovery task must be completed. |
| Configuration item | Item or asset that is recovered in this task. |
| Description | Brief note about the recovery task. |

**Note:** You can create a recovery task at the recovery strategy level and also at the plan level.

**b.** Click **Create**.

Recovery task grid

All recovery tasks that you have created for the plan appear in a grid. You can group the recovery tasks based on the fields in the recovery task table. Grouping helps you to group the recovery tasks the way you want, focus, and manage the task groups.

**Note:** To group by a field, you must set up the group criteria value as a BCM admin by selecting the **Group recovery tasks** option and a value in the **Group by** field of the plan template before creating the plan.

Dependencies

The dependencies column displays recovery tasks that match the asset scope level and the plan level. However, If it is at scope level, then it displays recovery tasks that match the scope level and also tasks that do not have a scope.

If it is at the Plan level, then the recovery tasks that match only at the plan level are displayed. Considering that the plan level recovery task does not have any scope.

If there is a cyclic dependency between tasks, then those recovery tasks are not displayed in the **Dependencies** column.

Task group

Groups the tasks based on the **Group by** field in the plan template.

**7.** To edit the data in a cell, double-click and click again in the cell.

**8.** To apply grouping and filter, click the vertical ellipsis icon.

Sort

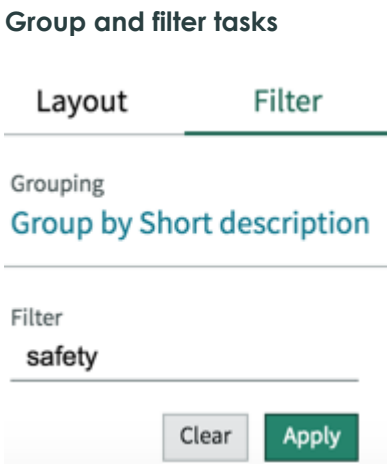
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can sort the data at each column level. The first click in the column header sorts the data of the column in ascending order ( ). The next click makes the sort descending ( ). Another click removes the sort.

Filter

Apply column filter to filter data that have simple text. For example, you can filter tasks with short descriptions that talk about safety.

Use the simple number filter to filter time critical data. For example, you can apply the filter to the **Completion deadline** column to filter the tasks that have to be completed within an hour of a business disruption.




9. To remove the filter, click the **Clear** button.
10. To delete one or more recovery tasks, select the record or records and click the **Remove** button.

### View the general details of a business continuity plan

Use the **Details** tab of the plan to view the general information about the template that is used for the plan, its type, and other details.

#### Before you begin

Role required: sn_bcm.admin, sn_bcm.program_manager, or sn_bcm.planner

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon ( ).
3. Click **In Draft** state in the Planning list.
4. Click the link to the plan record in the **Name** column.
5. Click the **Details** tab of the business continuity plan (BCP).
   This tab gives you a summary of the plan details. You can edit the information if required.
6. Click **Save** after updating the plan details.
7. To generate a PDF and download a copy of the BCP to your local hard drive, click **Generate PDF**.
   A message appears with a downloadable link to the BCP PDF.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** After the plan is approved, the PDF is generated and attached to the plan.

8. To move a plan from **Approved** to **Draft** state, select the **Edit** button.
9. To create a copy of the plan, click the **Copy** button.
   If you have the permission to edit a BIA, then you can also copy the BIA. A BCM planner and program manager can delete a plan and its related table records when the plan is in Draft, In Review, and Returned states. BCM admin can delete a plan irrespective of its state.

   a. Enter the name of the new plan in the Copy plan pop-up.

   b. Click **Confirm**.

   - The copy action creates an exact replica of the plan with the name that you enter in the Copy plan pop-up. The copied plan is moved to **Draft** state.
   - The action copies the plan assets, plan documentation sections, recovery teams, loss scenarios, its related asset dependencies and recovery strategies, and recovery tasks of the original plan to the copied plan.
   - The documentation sections of the copied plan are in **Pending** state. Edit each section, if required, and move it to **Complete** state.
   - Dependencies are populated when the plan is copied.

### View approval state flows for a business plan

View the approval state transitions sent at each level of the approval process, and the details of the approvers as you direct the business plan through multiple levels of approvals.

#### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager, sn_bcm.viewer

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon (  ).
   You can view approval records for a business plan that is any state except **Draft** and **In Review** states.
3. Click the link to the business plan record in the **Name** column.
4. To view the approval details of the plan, click the Approvals related list.
   If there are no approval records in requested state for the plan, then you can either **Reject** or **Approve** the plan.
5. Click the link to the approval record in the **Name** column.
   You can view the name of the approval, approval level, its current state, and the details of approvers such as users and groups.
6. To view the approval history of the plan, click the **Details** tab.

   a. Click the Approval History related list.
   You can view the complete approval history with details of the approvers and the date and time of its creation.

   State transitions for multiple levels of plan approvals:

   Not Yet Requested

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

State where an approval is not yet sent to the approvers at a respective level.

Requested

Approvals are sent to the approvers of that level. Correspondingly, the state of all successive levels of approvals turns to Not Yet Requested.

Approved

One or more approvers have approved the plan at the respective level. Correspondingly, the state of the succeeding level of approval moves to Requested.

Rejected

One or more approvers have rejected the plan at a particular level. Correspondingly, the state of all succeeding levels of approvals moves to No Longer Required.

No Longer Required

If the approvers at a level have rejected the plan, then the state moves to No Longer Required for all succeeding levels of approvals.

## Structured workflows for Exercise and Crisis Management

Business Continuity is an ongoing set of activities aimed at reducing the risk of an organization and improving its ability to respond to and recover from disruptions. To this effect, recovery and exercise management helps in continuous testing and improving of your continuity plans, and minimize business disruptions when a crisis strikes.

The objectives of Recovery and Exercise Management are:

Plan Exercising Recovery Management

- Provide continuous testing and improving of continuity plans.
- Improve effectiveness and usability of plans during simulated and actual crisis events.

Crisis Management

- Minimize unavailability of critical business functions and processes across the organization.
- Minimize financial, reputation, legal, and regulatory impacts during a crisis event.

### Start an exercise event

Create an exercise event to test your business continuity and recovery plans on a planned date and monitor the completion of the event tasks.

#### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the **Start an Exercise** link in the **Actions** section of the workspace.
3. On the modal form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create Exercise form

| Field | Description |
|---|---|
| Short description | Name of the exercise event. |
| Assigned to | Auto-populates the name of the user who created the exercise event. As a BCM program manager you can update the field. |
| Exercise Method | Method to implement the event. The methods can be Simulation, Tabletop, or Walkthrough.<br>◦ Simulation: An environment that simulates an actual disaster with necessary equipment, supplies, and personnel.<br>◦ Tabletop: An exercise done in a room with a team analyzing over the plan, looking for gaps.<br>◦ Walkthrough: Each member of the team walks through a component of the plan in detail to identify weaknesses.<br>◦ Functional: Option to include ad hoc tasks that are not part of a plan. |
| Planned Start | Planned start date of the exercise event. |
| Description | Detailed description of the exercise event. |

4. Click **Submit**.
   The exercise event is created and is in **Pending** state.

### Start a crisis event

Unlike an exercise event, a crisis event strikes suddenly. Your business must be equipped to face the challenge and must be able to recover the critical business functions quickly to save you from business loss.

#### Before you begin
Role required: sn_bcm.planner, sn_bcm.program_manager

#### About this task
You may not have a plan ready for a crisis as it strikes suddenly without prior notice. However, you can have an event ready and add tasks to the crisis event depending on the requirement.

#### Procedure
1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the **Start a Crisis Event** link in the **Actions** section.
3. On the modal form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

#### Report Crisis Event form

| Field | Description |
|---|---|
| Short description | Name of the crisis event. |
| Assigned to | Auto-populates the name of the user who created the crisis event. As a BCM program manager you can update the field. |
| Description | Detailed description of the crisis event. |

4. Click **Submit**.
   The crisis event is created and is in **Pending** state.

### Review event details and start an exercise event

Review the details of an event in the **Details** tab, start an event to test your business continuity or recovery plan, and monitor the event's completion.

## Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager

## Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon (  ).
3. Click the **Pending** state in the Exercises list.
4. Click the link to the event record in the **Number** column.
5. Review the exercise event details in the **Details** tab and update if required.

#### Details for an exercise event

| Field | Description |
|---|---|
| Event | |
| Short description | Brief description about the event. |
| Event Type | Auto-populates the event type |
| State | Current status of the event. |
| Assigned to | Event coordinator to manage and complete the event. |
| Description | Detailed description of the event. |
| Planning | |
| Planned Start | Planned start date of the event. |
| Plan Approvers | Approvers of the event exercise. |
| Result Approvers | Person who approves the result of the plan. |
| Scope | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Exercise Method | Method to implement the event. Autopopulates the exercise method previously selected. |
| Goals | Goals to achieve from the exercise event. |
| Objectives | Objective of the event. |
| Results | |
| Actual start | Actual start date of the exercise. |
| Actual end | Date on which the exercise was completed. |
| Closed on | Date on which the exercise event was closed.<br><br>The field appears when the event is moved to closed state. |
| Result | Outcome of the exercise. |
| Result Summary | Summary of the exercise event. |
| Recommended Improvements | Recommendations on how to improve the exercise event. |
| Activity | |
| Work notes | Additional information about the exercise event. |

**Note:** You cannot view the **Results** section in **Pending** state. However, you can view the section in all other states.

6. Click **Save**.
   The event is in **Pending** state.
7. Click **Start event** for the exercise after you have updated the details.
   When you start an exercise, the **State** field moves to **Work in Progress** state. As a result approver, you can update the actual start and end dates of the exercise if the exercise was not conducted on the planned date. Update the outcome or the result of the exercise. The result can be Successful, Successful with Issues, or Unsuccessful. Enter the result summary and recommended improvements that can be followed for future exercises.
8. If all the activated plans of the event tasks for the exercise event are completed, click the **Submit for Approval** button.

   You must enter the **Actual start** and **Actual end** dates before submitting the exercise event for approval. Update the details in the **Results** section. Save the form after you make the changes and before submitting it for approval.

   Pending Approval

   When you click **Submit for Approval**, the event is set to **Pending Approval** state. In this state, you can only update the **Work notes** field.

   If there are any approval rules configured for the event, then approvals are generated and sent to the approvers. If there are no approval records in

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the requested state for the event, then you can either **Reject** or **Approve** the event.

You can view the approval details in the Approvals related list with its name, level of approval, and the state of the approval.

Select the Approval History related list to view the approval state, name of the approver, event number, the date on which the approval was requested, and comments if any.

**Note:** If you are a BCM Program Manager, then you can see the **Approve** and **Reject** buttons.

Returned

When the event is rejected, the state is set to **Returned** state. It can be moved to **Submit for Approval**, **Closed Complete** or **Closed Incomplete** states. Since this is related to an event, only certain sections like description, results, and work notes can be updated in the form.

When the event is in **Returned** state, you can edit the state of the event asset.

From the **Returned** state onwards, you can only add comments and attachments to the event task.

Closed Complete and Closed Incomplete

You can set the event state to either **Closed Complete** or **Closed Incomplete** by clicking the **Close Event** button.

Approved

When the event is approved, the state is set to **Approved** state. You can set the event state to either **Closed Complete** or **Closed Incomplete**.

9. To generate a PDF, click **Generate PDF** button and download the PDF.
   If you have edit access to the exercise event, you can save a copy of the event in PDF format to your local hard drive.

**Note:** By default, the PDF is generated and attached after the event is closed.

### Manage a crisis event

Review and update the details of a crisis event in the **Details** tab. Get the event ready for a crisis that may strike and disrupt your business.

#### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon (  ).
3. Click **Pending** state in the Crisis Events list.
4. Click the link to the event record in the **Number** column.
5. Review the crisis event details and update if required.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Details for a crisis event**

| Field | Description |
|---|---|
| Event | |
| Short description | Name or description of the event. |
| Event Type | Autopopulates the event type |
| State | Current status of the event. |
| Assigned to | Event coordinator who manages the crisis. |
| Description | Detailed description of the event. |
| Additional Information | |
| Actual start | Actual start date of the crisis event. |
| Actual end | Date on which the crisis event ended. |
| Closed on | Date on which the event was closed.<br>The field appears when the event is moved to closed state. |
| Activity | |
| Work notes | Additional information about the crisis event. |
| Compose | |
| Work notes (Private) | Additional information about the crisis event. |

6. Click the **Browse** button to add any document as an attachment.
7. Click **Save**.
   The event is in **Pending** state.
8. To start the crisis event, click **Start Event** button.
   After you start the event, it moves to **Work in Progress** state.
9. If all the activated plans of the event tasks for the crisis event are completed, click **Submit for Approval** button.

   You must enter the **Actual end** date and save the form before submitting the event for approval.

   Pending Approval

   When you click **Submit for Approval**, the event is set to **Pending Approval** state. In this state, you can only update the **Work notes** field.

   If there are any approval rules configured for the event, then approvals are generated and sent to the approvers. If there are no approval records in the requested state for the event, then you can either **Reject** or **Approve** the event.

   You can view the approval details in the Approvals related list with its name, level of approval, and the state of the approval.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Select the Approval History related list to view the approval state, name of the approver, event number, the date on which the approval was requested, and comments if any.

**Note:** If you are a BCM Program Manager, then you can see the **Approve** and **Reject** buttons.

Returned

When the event is rejected, the state is set to **Returned** state. It can be moved to **Submit for Approval**, **Closed Complete** or **Closed Incomplete** states. Since this is related to an event only certain sections like description, results, and work notes can be updated in the form.

When the event is in **Returned** state, you can edit the state of the event asset.

From the **Returned** state onwards, you can only add comments and attachments to the event task.

Closed Complete and Closed Incomplete

When the event is approved, the only option available is to close the event. You can set the event state to either **Closed Complete** or **Closed Incomplete** by clicking the **Close Event** button.

Approved

When the event is approved, the state is set to **Approved** state. You can set the event state to either **Closed Complete** or **Closed Incomplete**.

10. To generate a PDF, click **Generate PDF** button and download the PDF.
    If you have edit access to the crisis event, you can save a copy of the event in PDF format to your local hard drive.

**Note:** By default, the PDF is generated and attached after the event is closed.

### View event details and monitor event task completion

View the event details and add impacted items to start an event.

#### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. To update an active exercise or crisis event from the Home page of the Business continuity workspace, click the link to the event record in the **Event** column of the **My exercises** section.
3. To update the event from the lists view of the workspace, click the lists icon ( ).
4. If the record is an exercise event and is in pending state, Click **Pending** link in the Exercises list.
5. Click the link to the event record in the **Number** column.
6. Review the event details in the **Details** tab.

   You can view and update all the details of an event. However, you cannot edit the event type.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A crisis manager should be able to report a crisis event with the information provided in the details tab. For more information, see Manage a crisis event.

7. Click the **Impacts** tab to add impacted items.
   To add a list of impacted items and activated plans to the event, see Add impacted assets and plans to an event.
8. Click **Event Tasks** tab.
   This tab appears for all crisis events but exercises that are of **Functional** type events only.

   The Plans section, which appears as a side panel, displays all the activated plans that are added to the event.

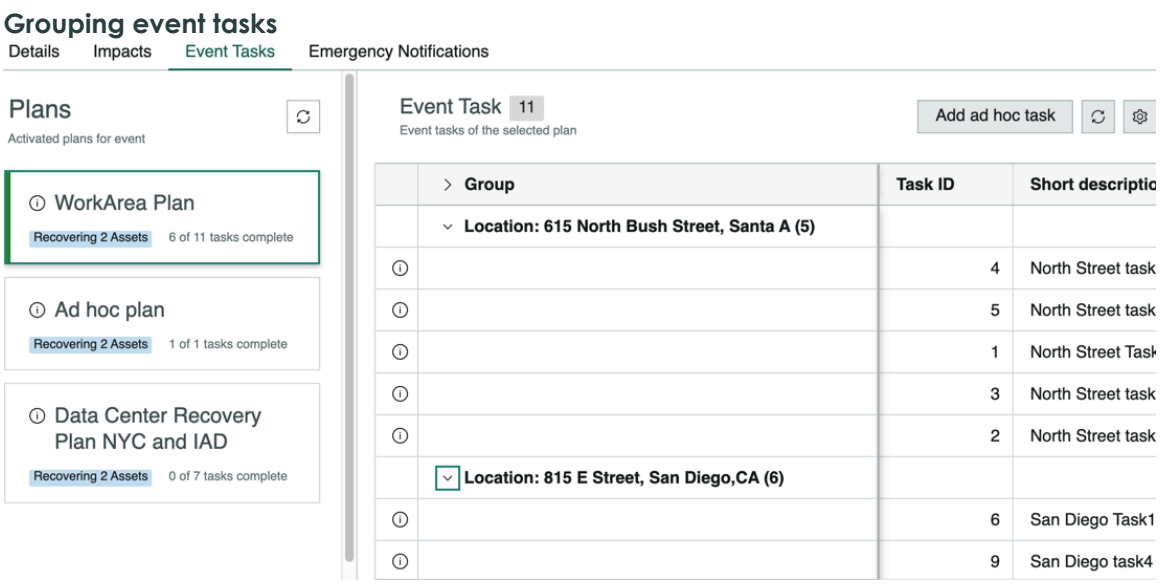
   When a plan is activated, all the recovery tasks where the scope is empty and tasks where the scope match with the impacted asset of the plan that is activated are added as event tasks for that activated plan.

   Each activated plan is an interactive card that shows you the number of assets that are in the process of being recovered and the number of event tasks that are completed for that activated plan. When you add an activated plan to the event task, all the recovery tasks of the plan are added as event tasks to the event.

   You can also create a task for the event that is not covered in any of the existing plans for the event as an ad hoc task.

   a. Click an activated plan card to view the associated event tasks.
      The selected activated plan card is highlighted in green and displays all the event tasks for that plan in a grid on the right pane.

      If the plan is pre-grouped, then the event task is also pre-grouped. Use the first column of the grid, which is the task Group column, to view the pre-grouped event tasks.




**Note:** If the activated plan refers to a different plan to recover a related asset, then all those related plans are listed below the main activated plan as **Related plans** in the left pane.

For more information on the planning and execution of a recovery event, see Data flow, planning, execution, and recovery of related plan assets in event.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**b.** To add an ad hoc task to the event, click the **Add ad hoc task** button.

**Create New Event Task form**

| Field | Description |
|---|---|
| Short description | Brief note about the event task. |
| Task ID | Defaults to the next number of existing event tasks for the plan. |
| Assignment group | Group to which the event task is assigned. |
| Assigned to | User or users from the Assignment group. If **Assignment group** field is empty, then select any user. |
| Additional assignee list | Additional users. |
| Impacted assets | Assets that are impacted for the event task. |
| State | Defaults to **Pending** state. |
| Dependencies | For tasks copied from plan level, dependencies are copied from plan recovery task. Dependencies cannot be added for ad hoc tasks. |
| Description | Information about the event task. |
| Activity | |
| Work notes | Information about the event task shared internally. |

**c.** Click **Save**.

**Note:** You cannot create an ad hoc task for activated plans that are in **Closed Complete** or **Closed Incomplete** state.

**d.** To update an existing event task, click the ⓘ of the task in the grid.

**e.** Update the **Actual start** and **Actual end** dates for the event task.

**f.** Update the assignment fields, if required.

**g.** Enter any event task related information in the **Work notes** field of the **Activity** section.

**h.** Click **Save**.

Calculation of actual duration and total effort to recover an event asset:

Actual duration to recover an event asset is calculated by `Actual end – Actual start of an event asset`

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- the actual start of an event asset is the minimum start time of the event task executed for the event asset that is, event task that has the event asset as impacted asset. And the minimum start time of the activated plan without a task.
- the actual end of an event asset is the maximum end time of the event task executed for the event asset that is, event task that has the event asset as impacted asset. And the maximum end time of the activated plan without a task.

Total effort of an event asset is calculated by rolling up the actual time taken by all the event tasks that are executed for the event asset that is, the impacted asset in event task that contains the event asset. And the total effort of all activated plans associated with the asset without a task.

Actual duration of an event task

The difference in time between the actual start and actual end time.

Actual duration of an activated plan with a task

The difference between the actual start and actual end of the activated plan, where

- the actual start of an activated plan is the minimum start time of the event task for that plan
- the actual end of an activated plan is the maximum end time of the event task for the plan

Actual duration of an activated plan without a task

The difference between the actual start and actual end of the activated plan.

Total effort of an activated plan with a task

Sum of the actual durations of all event tasks that belong to the plan.

Total effort of an activated plan without a task

The difference between the actual start and actual end of the activated plan.

State transitions of an event task:

Open

When an event is started, its event tasks that do not have a dependent recovery task move to the **Open** state.

Pending

The event tasks that are dependent on other recovery tasks are in **Pending** state when the event is started. After the dependent tasks are closed, the parent event task moves to **Open** state.

Skip Task

This button is available only if you have logged in as a BCM program manager. **Skip** button appears when the task is in **Pending** or **Open** state and the event must be in Work in Progress state. Clicking **Skip Task** moves the task to **Closed Skipped** state. The actual start and actual end time at this state are blank.

Trigger

This button is available only if you have logged in as a BCM program manager. The task is in **Pending** state. Clicking **Trigger** moves the task to **Open** state irrespective of its dependencies.

Work In Progress

The task is in **Open** state. Clicking **Work In Progress** button moves the task to **Work in Progress** state. You can update the actual start time of the task in the

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Actual start** field in this state. If you do not update the actual start, the current date and time is recorded as the actual start time. The next available options are **Closed Complete** or **Closed Incomplete** state.

Closed Complete

The task is closed and complete. Actual end time of the task is recorded in the **Actual end** field. If you do not update the actual end, the current date and time is recorded as the actual end time.

Closed Incomplete

Actual end time of the task is recorded in the **Actual end** field. If you do not update the actual end, the current date and time is recorded as the actual end time. Update necessary information in the **Work notes** field and save the task.

### Add impacted assets and plans to an event

Quantify the performance of your continuity and recovery plans by tying it to an event and putting it to a test. You can measure the plan's success by the successful completion of the event tasks attached to the plans.

#### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager

#### About this task

A good business continuity plan is a result of thoughtful assessment of business impact analysis and the risks involved in a disruptive situation. However, the plan becomes viable only after it is tested in an event.

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. To update an active exercise or crisis event from the Home page of the Business continuity workspace, click the link to the event record in the **Event** column of the **My exercises** section.
3. To update the event from the lists view of the workspace, click the lists icon ( ).
4. If the record is an exercise event and is in pending state, Click **Pending** link in the Exercises list.
5. Click the link to the event record in the **Number** column.
6. Click the **Impacts** tab to view the list of impacted items.
   You can add assets, activated plans for the recovery of the assets, and an ad hoc plan for an event asset.
7. Click the **Impacts** tab to view the list of impacted items.

   Impacts grid displays impacted assets and activated plans. You can:

   - add the assets that are impacted and the plans that are related to the assets
   - view the plans related to the assets under the respective assets in the grid
   - add an ad hoc plan that does not have a plan reference
   - view the details of asset recovery and the activated plan by clicking the information icon ( )

   For information on the logic behind the calculation of recovery task entities, see Calculation of actual duration and total effort to recover an event asset.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If the impacted assets are CMDB CI data that came into the BIA automatically based on CMDB dependencies and when these assets are scoped in the plan, then at the time of recovery of the asset, the related assets and the related plans are automatically pulled into the exercise event as impacted assets and activated plans in the **Impacts** tab.

For more information on the planning and execution of a recovery event, see Data flow, planning, execution, and recovery of related plan assets in event.

8. Click the **Add assets** button to recover assets in the event.

   a. Select the impacted item type or the primary element to recover in the Add Assets pop-up.

   b. Click **Next**.

   c. Select the impacted items or assets in the Add Assets pop-up.

   d. Click **Save**.
   The grid displays the assets in the **Short description** column. As these assets are added to the event, they are now event assets. The grid also displays the state of assets whether they are recovered or not, and the actual time taken for recovery.

9. Click **Add plans** button.
   The assets can be part of an approved plan or without a plan.

   Use the grouped button to add as many plans as you need to an event. However, you can add only one ad hoc plan to the event. **Add ad hoc plan** button appears when an ad hoc plan is created for an event. This ad hoc plan is the one that appears in the Ad hoc plan pop-up when you select assets.

   Add ad hoc plan button is shown after an adhoc plan is created for an event. The same is mapped to the selected assets in the ad hoc plan modal.

   - To select a plan that the impacted asset is part of, select **Show plan for impacted assets**.

     a. Select the asset that is impacted in the **Select Impacted Asset** field.

     b. Click **Next**.

     c. Select the plans for the impacted asset in the Select Plans to Add pop-up.

        This action creates the activated plan if it does not already exist and then maps the impacted asset with the activated plan in the Impacted Asset to Activated Plan [sn_recovery_impacted_asset_to_activated_plan] table.

   - To display all plans and select assets from the plans, select **Show all plans**.

     a. Click **Next**.

     b. Select plans from the list in the Select Plans to Add modal.

     c. Click **Next**.

     d. Select impacted assets for the selected plans from the Choose Assets of Selected Plans modal.

        This action adds impacted assets, activated plans, and maps the impacted assets with the activated plans in the Impacted Asset to Activated Plan [sn_recovery_impacted_asset_to_activated_plan] table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

As the plan is being activated for the event that is active, the plans or the assets cannot be removed once the event is **In Progress** state.

**e.** Click **Confirm** to proceed with the activation of the selected plans. This message pops up for the events that are **In Progress** state.

**Note:** The impacted items or event assets, the activated plans, and their status are displayed in the grid.

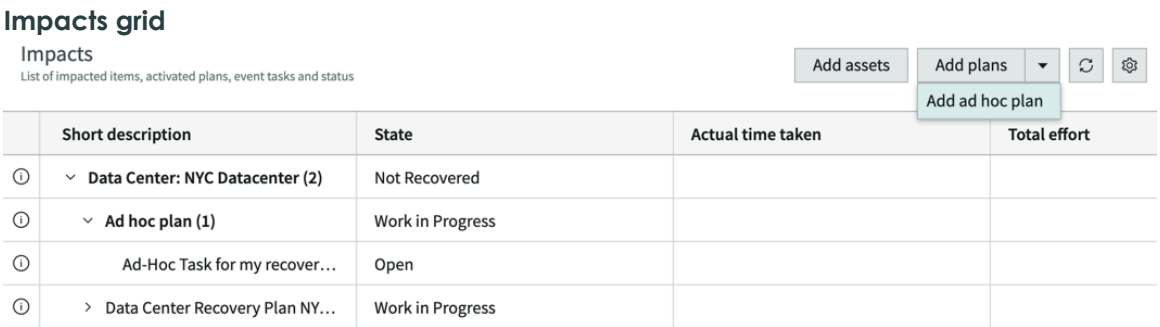
**10.** Click the **Add ad hoc plan** button.
After you add assets to the event, you can click the **Add ad hoc plan** button to add an ad hoc plan for the selected assets of the event.

**Note:** This action adds an ad hoc plan if it does not already exist for the event. After an ad hoc plan is added to the event, subsequently whenever you click the add ad hoc plan button, all the impacted assets that you select are added to this existing ad hoc plan.

There can be only one ad hoc plan per event.

- You can delete the impact of an event that is its assets, activated plans, and tasks until the event begins or is in **Pending** state.
- If the exercise or the crisis event is in **Work in Progress** state, then you cannot delete the associated impacts.
- You cannot add event assets, activated plans, or event tasks when the event is in **Closed Complete** or **Closed Incomplete** states.

You can view the selected assets and plans in a hierarchy on the grid in the **Short description** column.

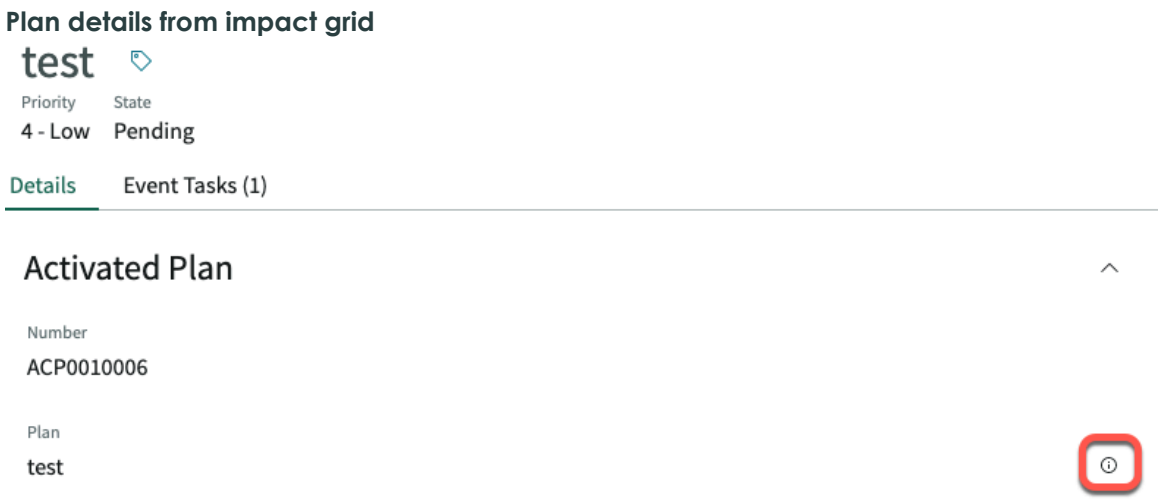



**11.** To update the impact details, click ⓘ of the respective record to launch the event asset and activated plan in the form view.

**a.** To view the plan details of an activated plan, click ⓘ for the respective plan record in the impact grid.
You can view the activated plan number, the plan name, its short description, state of the plan, priority, and description details.

**b.** Click the **Open Record** link next to the plan name.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The action opens the plan in a separate tab, where you can view its complete details.

Editable details in an Impacted Asset

In the impacted asset details, you can only edit the **State** of the asset if it has been recovered or not, and the **Actual time taken** to recover the asset. However, the rest of the impacted asset details are view only.

Editable details in an Activated Plan

You can edit the state of the plan, its priority, and description. However, you cannot edit the activated plan number or its short description.

Editable details in an impacted Event Task

You can only edit the **Assignment group**, **Assigned to**, and **Additional assignee list** fields. The rest of the fields are read only.

12. Click **Save**.
13. Click the refresh icon ( ) to display the updated state of the asset or plan, and the actual time taken to recover the asset.

### Data flow, planning, execution, and recovery of related plan assets in an event

When the configuration item data is available on the Now Platform the same items can be used to assess dependencies in business impact analysis (BIA). The dependencies from the BIA can then be used in the planning and events. The configuration items (CIs) can be added manually to the plans and events as well.

You can also add new plans with assets to be recovered in a sequence.

The advantages of automatic data flow are:

- You can reuse the configuration item (CI) data that is created in CMDB in BIA, and from the BIA the dependencies are used in the plans and events.
- You have the capability to branch off to a related referred plan within the task of the main plan before executing the rest of the tasks in the main plan, especially when the referred plans are managed by planners of other departments or teams to recover their respective assets.
- The flow of execution is sequenced as per the Task ID and no event task is skipped in between.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Automatic data flow from CMDB to BIA and BIA to plans

When a record in created in Now Platform as a configuration item in CMDB, the record with all its related items are available for you to leverage as assets to assess dependencies in BIA.

CMDB

Data is created as a CI and the record is stored in CMDB. In CMDB, this CI is related to other items by a relationship either that depends on or used by the other related items. For example, if it's a Data Center NYC, then it can depend on SAP on-premise application and other web servers, business processes, locations, and others.

BIA

When you assess a BIA based on CMDB dependencies, the CMDB CI and its related items are automatically available as items for assessment in BIA. You can add these dependencies and the source of these items are tracked as CMDB. Therefore, the data created in CMDB is available as dependencies in BIA. In addition, you can also manually create other dependencies in BIA. For example, the Data Center NYC and its dependent SAP on-premise application are available in BIA to be added as dependencies. In addition, you can also add dependencies manually such as a Facility: New York.

Plan

When you are in the planning stage, if you have scoped the BIA-dependent item and added it as the scope, then the dependencies of the scoped item are available as Related Assets. Also, the plans existing for these assets are available as Related Plans. In addition, you can add new plans also. For example, a plan is created for Data Center: NYC, along with which the related plans of the related assets such as SAP on-premise application and Facility: New York (created in BIA) also move in to the planning phase automatically. In addition to the items that came from the BIA, you can also add new assets manually to the plan.

In the **Recovery Tasks** tab of a plan, you can also refer to a different plan and select the plan from the list of related plans.

Exercise

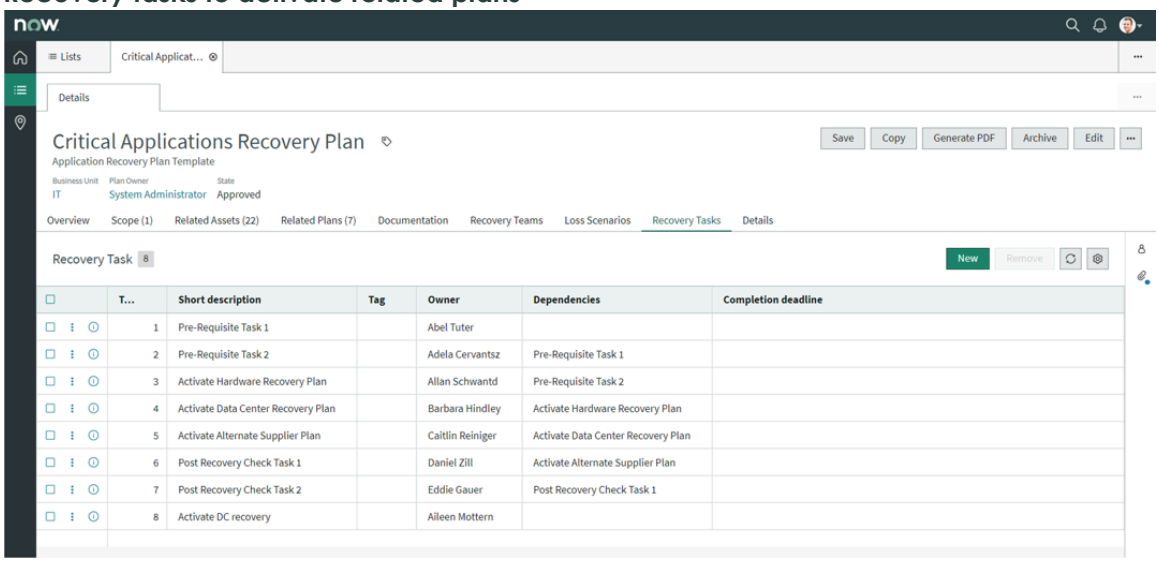
In the event, the impacted assets and the activated plans are pulled into the **Impacts** tab automatically based on the dependencies in the BIA. Along with the primary scope of exercise and related impacts, you can also add assets and plans manually, which are all pulled into the exercise for recovery.

## Planning phase

In this planning phase, as a planner you can identify the related assets, add the related plans, and set a sequence and dependencies for execution of recovery.

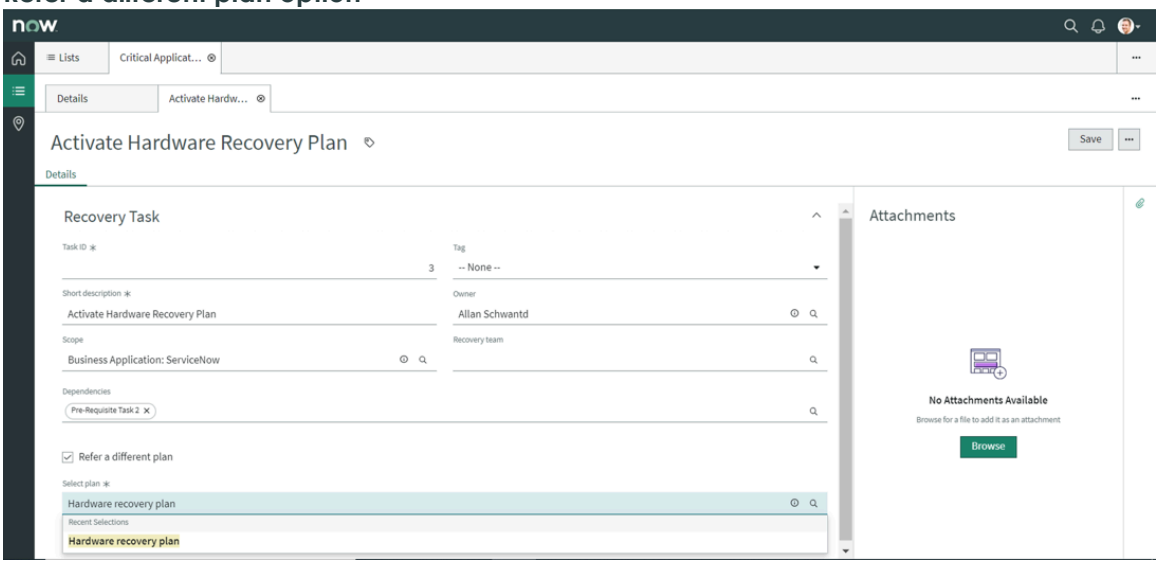
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Recovery tasks to activate related plans




If you must recover assets in Data center A before recovering assets in Data center B, then you can refer to a different plan that follows the recovery process of Data Center A. In this case, use the **Refer a different plan** option in the **Recovery Tasks** tab of the main plan, and select the relevant plan from the related plans to recover Data center A. The referred plan has its own set of tasks that the application executes when it comes to this particular task. You can also set a sequence for the execution of the referred plan within the event tasks of the main plan.

### Refer a different plan option

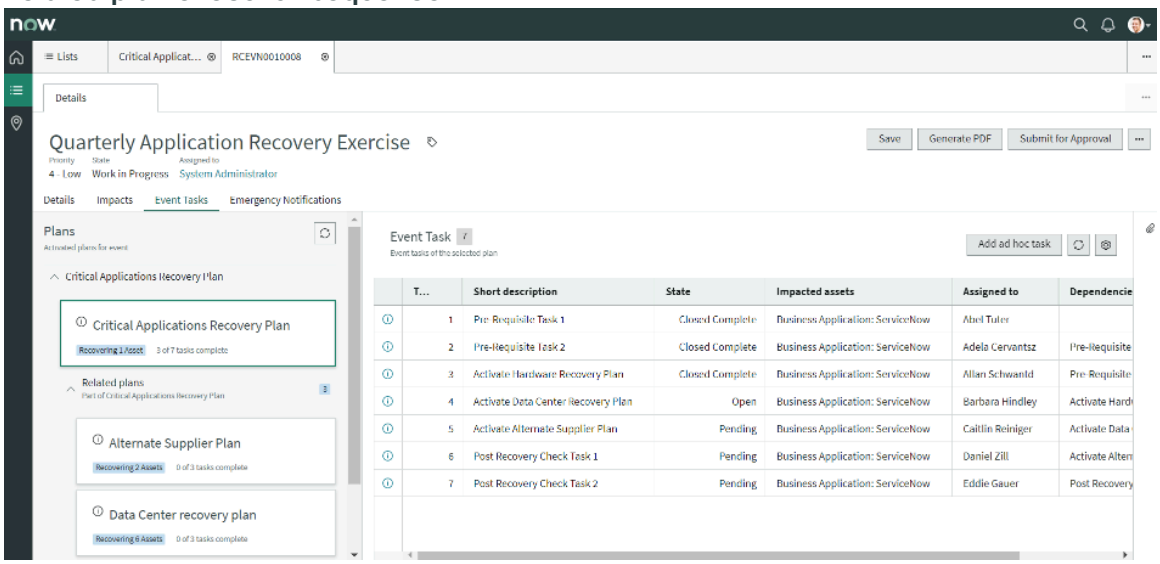



## Tracking and execution phase

In the tracking and execution phase, you can activate relevant plans during an event recovery. When you add an impacted asset in the **Impacts** tab of an exercise, then all the related assets and related plans are pulled in. Similarly, if you add a plan, then all its sub-plans are also added.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Related plan execution sequence




Navigate to the **Event Tasks** tab to track the execution of the event tasks of the selected main plan. When you click the **Start Event** button for an event, the tasks are triggered for execution. When you select the main activated plan in the **Plans** section of the left pane, you can view all the event tasks of the selected plan listed on the right pane as event tasks. In the **Plans** section on the left, below the main plan are the **Related plans**. The event tasks of the main plan are executed in the order of Task ID sequentially but when a particular task in the sequence has a referred or a related plan, then the application branches off to that plan and executes all the tasks listed in that plan thereof and completes the sequence before coming back to the original main plan from where it branched off to complete the rest of the tasks in the sequence. Therefore, there's a main list of recovery tasks under a main plan, within which there are sub-plans with their own set of recovery sub-tasks. The application executes all the tasks sequentially within the referred plan before it continues to execute the rest of the recovery tasks sequentially in the main plan.

**Note:**

For a primary main plan, if there are related referred plans within, then the application executes only the referred sub-plan but does not execute any other related plan that the sub-plan might have. The hierarchy of execution stops with the first level only if there are sub-plans.

### View your recovery tasks from Self-service

View the tasks assigned to you or a recovery task team that you are a part of to recover assets from a crisis or exercise (Functional type) event. Your BCM Program Manager assigns the tasks to you and you can view them any time you want from the self-service application menu.

#### Before you begin

Role required: sn_bcm.recovery_team_member

#### Procedure

1. Navigate to **Self-Service** > **My Recovery Tasks**.
2. View the list of event tasks assigned to you, the assigned group that you are part of, or a recovery team that you belong to.
3. Sort the **Event Type** column to list the crisis-related tasks at the top.
4. View the **Event Task type** column to understand whether it is planned or an ad hoc event.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click the link to the **Task ID** of an event task that you want to update.
   You can update the **Actual start** and **Actual end** details.
6. To add any notes to the event task activity, click the Activity related list and add the information in the **Work notes** field.
7. To update the task to in progress **State** field, click the **Work in Progress** button.
8. To close the task, click either **Close Complete** or **Close Incomplete** button.
   For more information, see State transitions of an event task.
9. Click **Update** after your changes.

## Crisis Management map

You can integrate the crisis management application with the Crisis Management map to receive alerts as the alert feeds on possible threats in continuing the business operations of your organization.

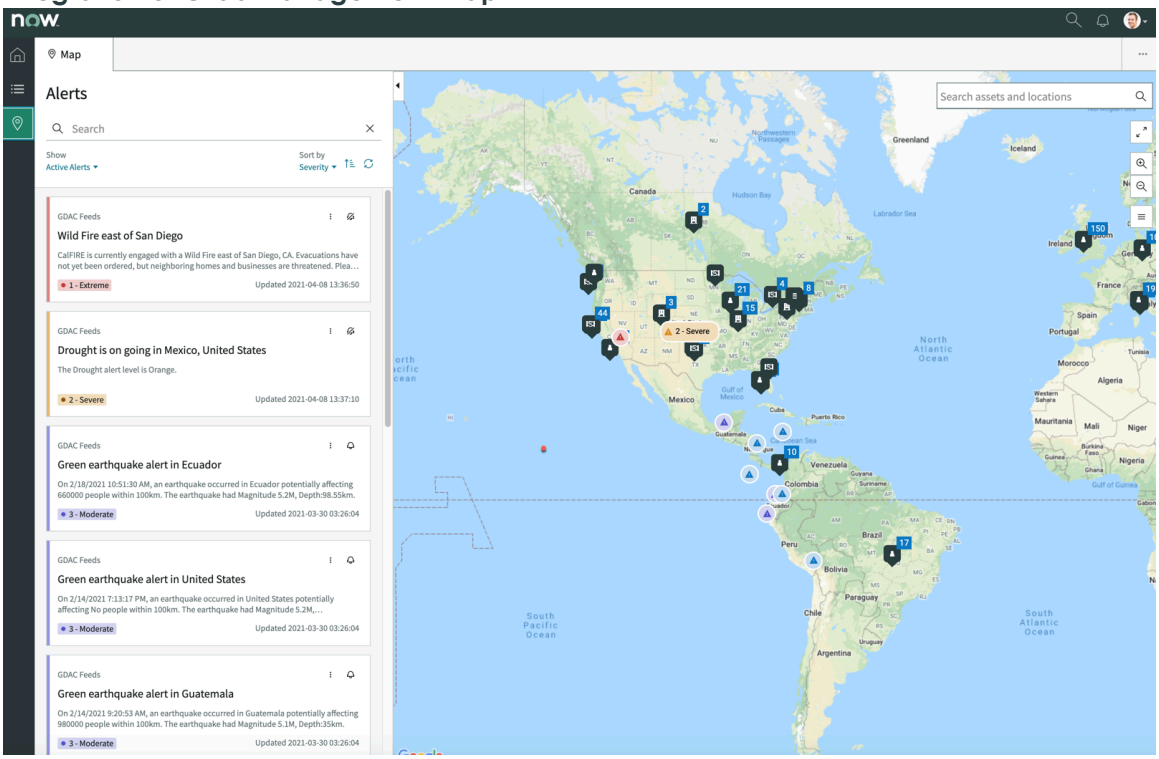
A threat feed is the data intelligence information of a potential or current threat that can pose a danger to an organization and stop its business routine or disable its business processes. Threat feeds can include but not limited to:

- Severe weather or tornado
- Hurricane
- Earthquake
- Wildfire or red flag warnings
- Flood
- Civil unrest or riots
- War or military conflict

As a BCM administrator, you can enable or disable threat feed integrations provided by the base system. You can also configure additional threat feeds in to the Crisis Management application. The integration and configurations that you set up alert the crisis manager of the threats and aid to take appropriate action on time.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Integration of Crisis Management map




### Setting up the crisis map

Before you integrate the crisis management map with the geographical locations of your assets, there are certain configurations that you must do to display the active alerts in the crisis map.

## Understanding feed, alert, and event

Feed

A feed is news content updated frequently and provided on a world-wide website. You can subscribe to a news feed by manually entering the web address or URL of the feed channel in the **Web** field of the Feed form.

Alert

An alert is a notification that reports an incident happened at a particular place and time. First, an incident or an event reportedly happens. Then, the alert triggers a notification that reports or notifies the incident to the concerned people to take an action.

Event

Based on the severity of the alerts, you can take actions by just notifying the stakeholders of the incident that happened or declare a crisis event. An event can become a crisis event if it disrupts the business operations. In such a case, you can run the Crisis Management workflow to activate the business continuity and disaster recovery plans for the locations impacted by the event.

## Setup steps to integrate crisis map

You require the following steps of configurations for the threat and alert feeds to show up in the crisis map visualization.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- To search locations on the crisis map, set up the system property.
- To manage your threat feed subscriptions sourced internally and externally, configure scheduled data imports.
- To plot your organization's assets or resources on the crisis map, configure the resources.
- To specify the conditions under which a feed should bubble up as an alert on the crisis map, configure alert rules.
- Finally, to act on a critical alert from the crisis map dashboard,configure an alert action.

### Configure search for places in crisis map

Set the system property to manage searching places on the crisis map.

#### Before you begin
Role required: Administrator

#### About this task
To enable crisis map functionality in the GRC: Crisis Map application, you must set up Google maps. For more information, see Set up Google Maps API.

**Note:** Prior to enabling the Crisis Map feature, ensure that you have purchased and set up Google Maps API.

#### Procedure
1. To open the System Properties table [sys_properties], enter sys_properties.list in the left pane of the application navigation filter.
2. Search for sn_bcm_map.use_google_places_lib in the **Name** column.
3. To search places in the Google map, set the value to **True** in the **Value** column for the sn_bcm_map.use_google_places_lib system property.

### Configure scheduled data imports for crisis map

Manage your subscriptions to threat feeds from internal or external sources by configuring scheduled data imports.

#### Before you begin
Role required: System administrator

You must set up the Google maps for enabling the crisis map functionality. For more information, see Set up Google Maps API.

#### About this task
Threat feeds provide a situational awareness of potential or current threats to an organization's security. Threat alerts can be weather alerts, pandemic alerts, geopolitical situations, or internal events like security incidents and system outages.

#### Procedure
1. Navigate to **Threat and Alert Data Feeds** > **Administration** > **Scheduled Imports**.
   Following two scheduled data imports exist within the base system.

| Name | Data source |
|---|---|
| GDAC Feed Source | GDAC Feeds |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Name | Data source |
|---|---|
| Weather.gov Severe Alerts Scheduled Import | Weather Gov Alerts |

2. To add a new scheduled data import, click **New**.
3. On the form, fill in the fields.

**Scheduled Data Import form**

| Field | Description |
|---|---|
| Name | Name of the scheduled import. Normally the source is the name. |
| Data source | Internal or external source of the threat and alert data used for import. |
| Run as | User who has the permission to import the threat alerts. |
| Active | Option for enabling the alert as active. |
| Application | Read-only field. The field helps distinguish items relevant to the crisis map. |
| Run | Frequency at which the data is imported. |
| Conditional | Option to indicate if a conditional script is required for the threat alert import. |
| Concurrent Import | Option for allowing concurrent imports. |
| Execute pre-import script | Option for enabling the execution of a pre-import script. |
| Execute post-import script | Option for enabling the execution of a post-import script. |

4. Click **Submit**.

### Configure a resource for crisis map

Configure resources to plot the organization's assets on the crisis map. The assets can be locations, employees, data centers, suppliers, and others. Configuring resources is also required as an input to set up alert rules.

#### Before you begin

Role required: System administrator

Set up the Google maps for enabling the crisis map functionality. For more information, see Set up Google Maps API.

#### Procedure

1. Navigate to **Threat and Alert Data Feeds** > **Administration** > **Resource Configurations**.
2. To add a new scheduled data import, click **New**.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Resource Configuration form**

| Field | Description |
|---|---|
| Name | Name of the resource configuration used in the map visualization. |
| Icon | Image representing a resource item on the map. |
| Table | Table for resources to plot on the map. |
| Location field | Location column of the table used as location on the map. |
| Use Coordinates | Option for enabling coordinates to plot the resources on the geo-map. |
| Application | Read-only field. The field helps distinguish items relevant to the crisis map. |
| Active | Option to indicate that the resource configuration is active. |
| Category | Value is BCM application. Helps to identify the BCM-related resources when multiple applications use the component. |
| Searchable | Option to indicate if the resource is searchable in the map visualization. |
| Contact User Field | Contact for communication for the resource in focus. |
| Contact Alias | Contacts for identification. |
| Display Fields | Fields selected for display as the contacts. |
| Conditions | Conditions for filtering records from the table. |

4. Click **Submit**.

### Configure alert rules to display alerts in crisis map

Set alert rules to specify conditions under which a feed has to be bubbled up and displayed in the dashboard as an alert. You can also specify the conditions under which an alert is no longer valid and dismiss it from the dashboard.

#### Before you begin

Role required: Administrator

#### About this task

Configure an alert to notify the crisis manager of an impending danger, potential harm, or risk that can cause business disruption. Set up filter conditions to notify events or feeds that can happen within a boundary from the location of your assets.

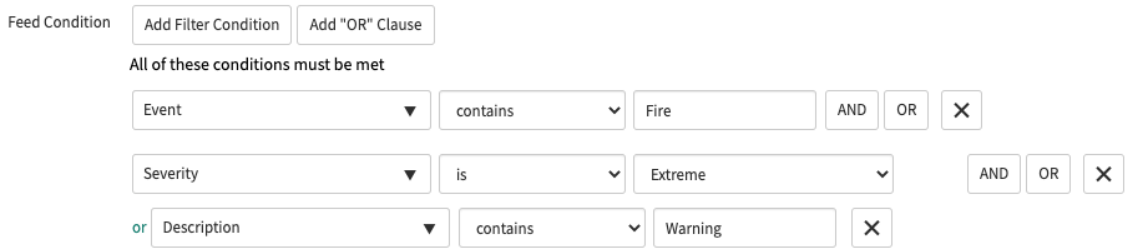
Configuring an alert rule: Define simple conditions to evaluate an alert rule and determine the feed items that generate an alert. These alerts are displayed on the Crisis Management map.

Feed condition filters

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use these filter conditions to set your rules for a feed alert. Setting filter conditions help you to filter those alerts that are critical to your business locations from the thousands of feeds that come from the feed resources you have subscribed. Business locations can be corporate offices, employee locations, data centers, suppliers, and others.

**Feed conditions**




Advanced condition script filters

Use the advanced rules option to set a filter rule with a condition script. For example, you can set a condition based on the proximity of the crisis to your asset locations. You can also make the rule active.

## Procedure

1. Navigate to **Threat and Alert Data Feeds** > **Administration** > **Alert Rules**.
2. Click **New**.
3. On the form, fill in the fields.

**Alert Rule form**

| Field | Description |
|---|---|
| Name | Name of the alert rule. |
| Active | Option to set the rule active. |
| Application | Read-only field. The field helps distinguish items relevant to the crisis map. |
| Order | Display order of the alert rule. By default it is 100. |
| Description | Details about the alert. |
| Create Condition | |
| If Resource Impacted | Option for enabling an alert rule if a resource is impacted. |
| Advanced | Option for enabling advanced filter rules with a condition script for the alert rule. |
| Optimize Impact Area | Option to indicate if the map area is to be optimized. Select the check box for optimal performance. |
| Feed Condition | Conditions to filter alerts based on the set rule. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Advanced Condition Script | This field appears if the **Advanced** option is selected. Enter a script to filter feeds based on a criteria, for example, active alerts. |
| Dismiss Condition | |
| When Feed Deleted | Option to indicate that the alert must be dismissed from the dashboard, if the feed is deleted. |
| When Resources Not Impacted | Option to indicate that the alert must be dismissed from the dashboard, if there are no resources impacted. |

4. Click **Submit**.

### Configure an alert action

The alert actions are the follow-up actions that you can perform from the crisis map dashboard.

## Before you begin

Role required: System administrator

## Procedure

1. Navigate to **Threat and Alert Data Feeds** > **Administration** > **Alert Actions**.
   You have the following two actions that are available within the base system.

| Name | Description |
|---|---|
| Notify | Used to send email notifications to stakeholders and the asset managers that are within the impact radius. |
| Declare Crisis | Used to declare a combination of alert and critical assets as a crisis event. |

2. To add a new alert action, click **New**.
3. On the form, fill in the fields.

### Alert Action form

| Field | Description |
|---|---|
| Title | Title of the alert action. |
| Description | Detailed description of the alert action. |
| Name | Name of the action in the crisis map dashboard. |
| Action name | Unique name for the alert action. |
| Run once | Option to indicate the execution of the action one or more times from the dashboard. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Type | Type of action to be executed. It can be a task, script, or flow. |
| Task type | Task type used for the action. |
| Application | Read-only field. The field is used as a flag to filter the items relevant to crisis management from a common list of actions. |
| Active | Option to indicate that the alert action is active. |
| Order | Display order to be followed on the dashboard. |
| Run automatically | Option for enabling the action to be executed automatically based on a condition. |
| Roles | User roles who can execute the task successfully. |
| Display Fields | Fields to be displayed in the response actions after the actions are executed. |
| Condition | Conditions to execute the actions. |
| Task script | Task script to be executed when the user clicks the action control on the dashboard. |

4. Click **Submit**.

### View and manage alerts in the crisis map interface

Business Continuity Management integrates with the Crisis Map to provide you the capability of identifying a threat and its geolocation from your asset locations.

#### Before you begin

It not only helps you to identify a threat as a business crisis but also notify your stakeholders and declare it as a crisis event if it has the potency to disrupt your business.

**Note:** Activate the Business Crisis Management Map (sn-crisis-map) application for the crisis map feature.

Role required: BCM admin or BCM Program Manager

#### About this task

Use the crisis map to manage feeds, prioritize alerts based on their severity, and create events. Thereafter, you can run the Crisis Management workflow and activate the business continuity and recovery plans for the locations impacted by the event.

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the map icon ( ).

   The alerts section is on the left of the workspace and the map view is on the right.

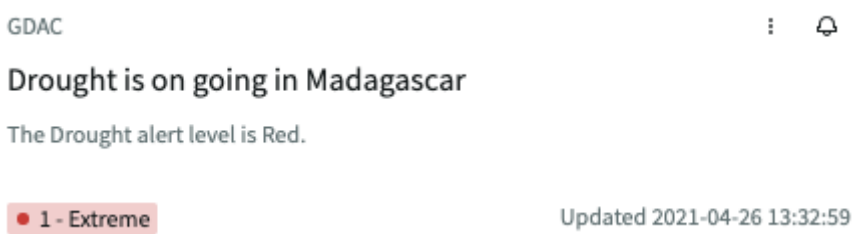
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Alert control feature | Description |
|---|---|
| Search Alerts | Key word to search and filter alerts from the list. |
| Select active or dismissed alerts | List to select either active or dismissed alerts. When an alert is dismissed, it becomes inactive. |
| Select column to sort by | List to select and display alerts based on their severity, created, or updated date. |
| Change sort order ( ) | Sorting order of the alerts, either in ascending or descending order. |
| Refresh Alerts ( ) | Option to refresh the alert list and the map components after an update. |

Threat alerts, based on severity or in any sorting order that you have set, are displayed in a list view. As you point to an alert in the list of alerts, you can view additional details about the impact of the threat.

Each alert record in the list has the following details:

**Alert record in the alert list**




Title
: Name of the alert.

Description
: Brief note about the impact of the alert.

Severity
: Intensity of the threat impact. It can be extreme, severe, moderate, minor, or unknown.

Updated details
: The alert's last updated date and timestamp.

3. Click an alert record to open the alert in its detailed view and view its corresponding impacted area on the map.
4. To go back to the list view of alerts, click the **Back** button.
5. To open the alert details in the form view, click the **Open Alert** option in the alert menu icon ( ).
   This action opens the record in a separate **Details** tab.
6. To go back to the alert list, click the **Map** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. If the alert does not pose a threat currently to your employee locations, datacenters, core companies, or any of your business establishments, click the **Dismiss Alert** option in the alert menu.
   If you know that the alert would not hamper your business operations, you can dismiss it in the list view as well as in its detailed view. When you dismiss an alert in the list view, it is removed from the list. If you dismiss an alert from the detailed view, the alert is removed and brings you back to the list view so that you can review the other alerts in the list. In both cases, you can see a confirmation message about the dismissal of the alert.

8. To subscribe to the alert notifications, click the subscribe icon ( ).
   You receive an email and workspace notifications every time the alert or its source feed item is updated.

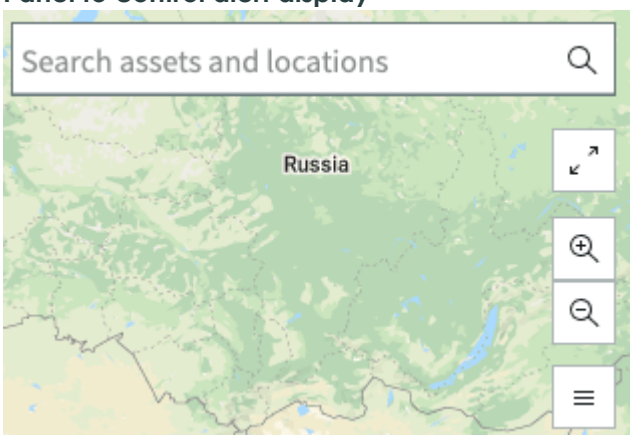
### Set controls to customize alerts on the map dynamically

Use a set of controls on the crisis map to display the alerts that are critical to your asset locations.

#### Before you begin
Role required: BCM admin or BCM Program Manager

#### About this task
You can customize the crisis map to display the layers that you would like to see on the map. Use the controls to view locations, employee locations, or core companies.

**Panel to control alert display**




The search bar helps you to search the assets and locations. A set of zoom controls helps you to zoom in and zoom out to focus on the area that has the information shown in that layer. The layers help you to get additional details on the map. Use the reset button to clear your control settings.

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the map icon ( ).

   The alerts section is on the left of the workspace and the map view is on the right.

3. Click the **Search assets and locations** field and enter a location or a datacenter that is impacted by an alert.
   When you search for a location, a mixed list of your company results with the display value of the records along with their icons, and the Google map pin icons appears.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you are not sure of both the employee locations or datacenters, then use the Layers control.

4. To change the zoom level of the map and view specific areas, use the zoom control buttons, zoom-in (  ) and zoom-out (  ).
5. To select and display the assets such as asset locations, datacenters, or core companies on the map, click the layers icon (  ).
6. To clear the map of all the search results, click the reset icon (  ).

### View resource layer clustering

View your assets or resources on the map.

#### Before you begin

Role required: BCM admin or BCM Program Manager

#### About this task

The layers that you see in the map like the assets, datacenters, and core companies are the resources that you have configured. Each of these layers fetches data from the respective resource tables. The assets, datacenters, and core companies resources retrieve data from the location, datacenter, and company tables, respectively.

Asset locations that are nearby to each other are clustered and a cumulative count of the assets is displayed next to the asset icon.

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the map icon (  ).
3. Click the layers icon (  ).

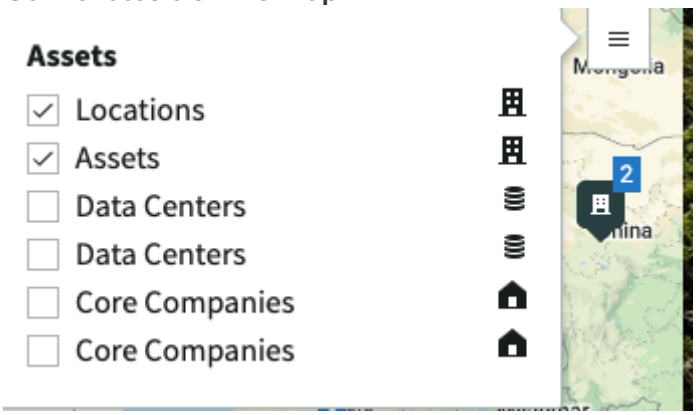
   The layers on the map appear just as pins on a Google map and are configurable. All the layer details like the asset locations, assets, datacenters, and core companies are displayed on the map by their configured icons.

   Use the layers control to view only the selected or all assets that can be toggled on and off on the map. As a crisis manager, when viewing the active alerts you can make an informed decision by concentrating on a single asset that can be critical at that moment from the rest.

4. To display a selective resource or asset on the map, select the check box of that asset.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Control assets on the map




The icons of the selected asset are displayed on the map. Layer icons are displayed within black borders, whereas alert icons are within a white circle.

5. Click an asset icon on the map to view its details.

   For example, if you click a datacenter icon ( ) that has no number or a count next to it, a pop over appears with the display information that you have configured in the Resource Configuration table [sn_fam_resource_config].

   If you have configured **Power** and **Power consumption** fields of the datacenter table [cmdb_co_datacenter] as the display fields in the Resource Configuration form, then the power consumption details of that datacenter are displayed on the pop over along with its location coordinates.

6. Click an asset icon with a number next to it.

   The map zooms in to show all the assets that match with the count in that cluster. You can further click each asset within the cluster and drill down to any asset to view its details on the pop over.

   You can view only one pop over at a time. The pop over disappears on clicking another node.

7. Click the reset icon ( ) to clear the search results on the map.

### View assets at risk within the impacted area

View the list of resources that are at stake because of an alert threat that is near your business locations. Take actions to protect your resources and prevent major loss.

#### Before you begin

Role required: BCM admin or BCM Program Manager

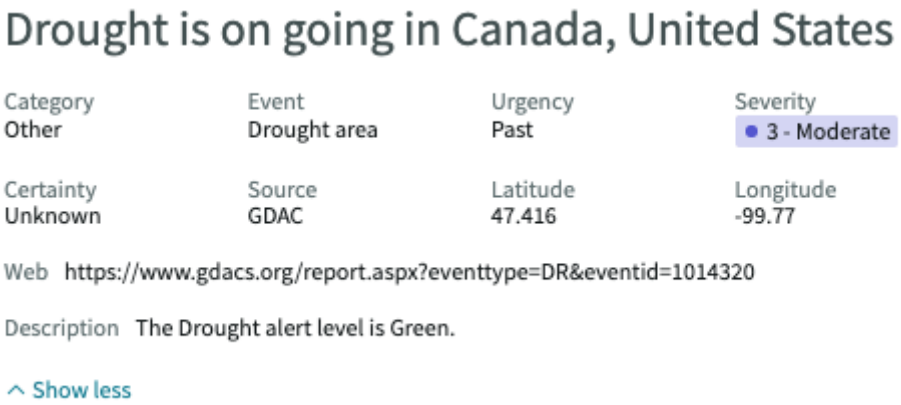
#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the map icon ( ).
3. Click an alert record to open the alert in its detailed view.

   You can see various details of the alert on the form header.

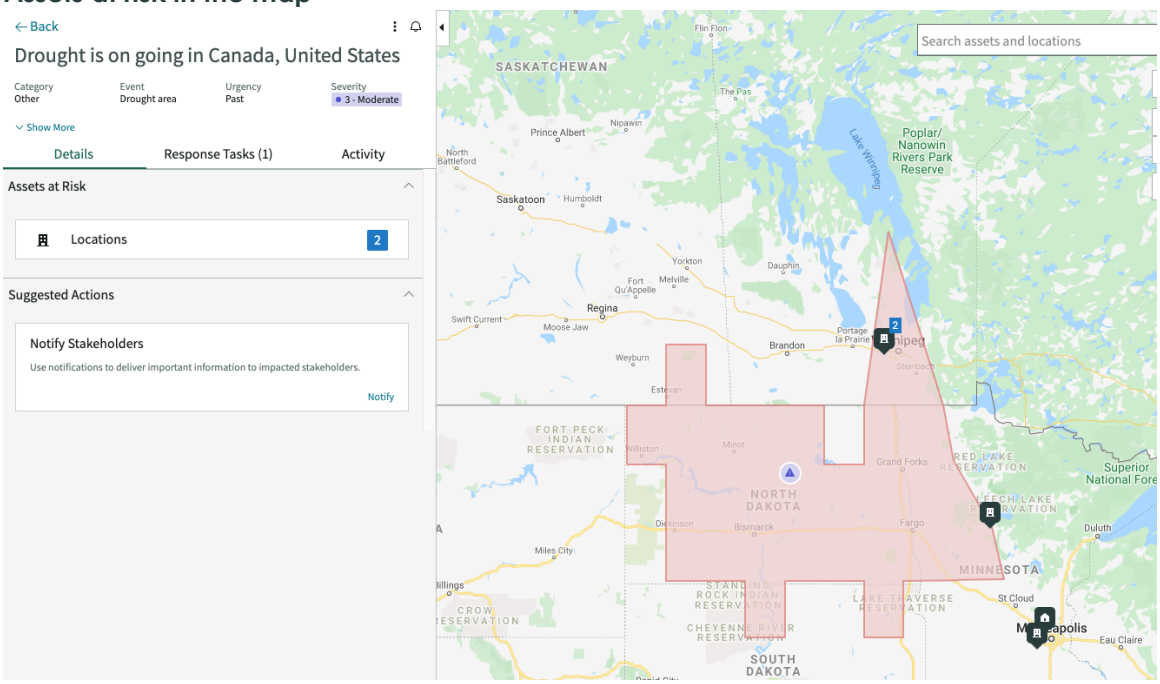
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Assets at risk form header**




- The title of the alert
- The category of the alert
- Urgency of the alert whether it is going to strike immediately or expected in future
- Its severity in terms of loss
- Its certainty as to how likely it can strike
- Source of the alert feed
- The coordinates of the impacted area
- The source or the website from where the feed alert was received
- Its description

**Assets at risk in the map**




4. Expand **Assets at Risk** section to view all the listed assets that are at risk.
   The **Assets at Risk** lists locations, datacenters, and core companies that lie within the impacted area of the alert. It also displays the count as to how many of these assets are

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

impacted. You can view the impacted area on the map and take any of the suggested actions.

The boundary of the alert's impacted area on the map is marked in mauve color. You can view the assets that are at risk within this impacted area on the map. If one of your location, datacenter, or a core company is impacted by the alert, you can edit the impacted zone to include the asset.

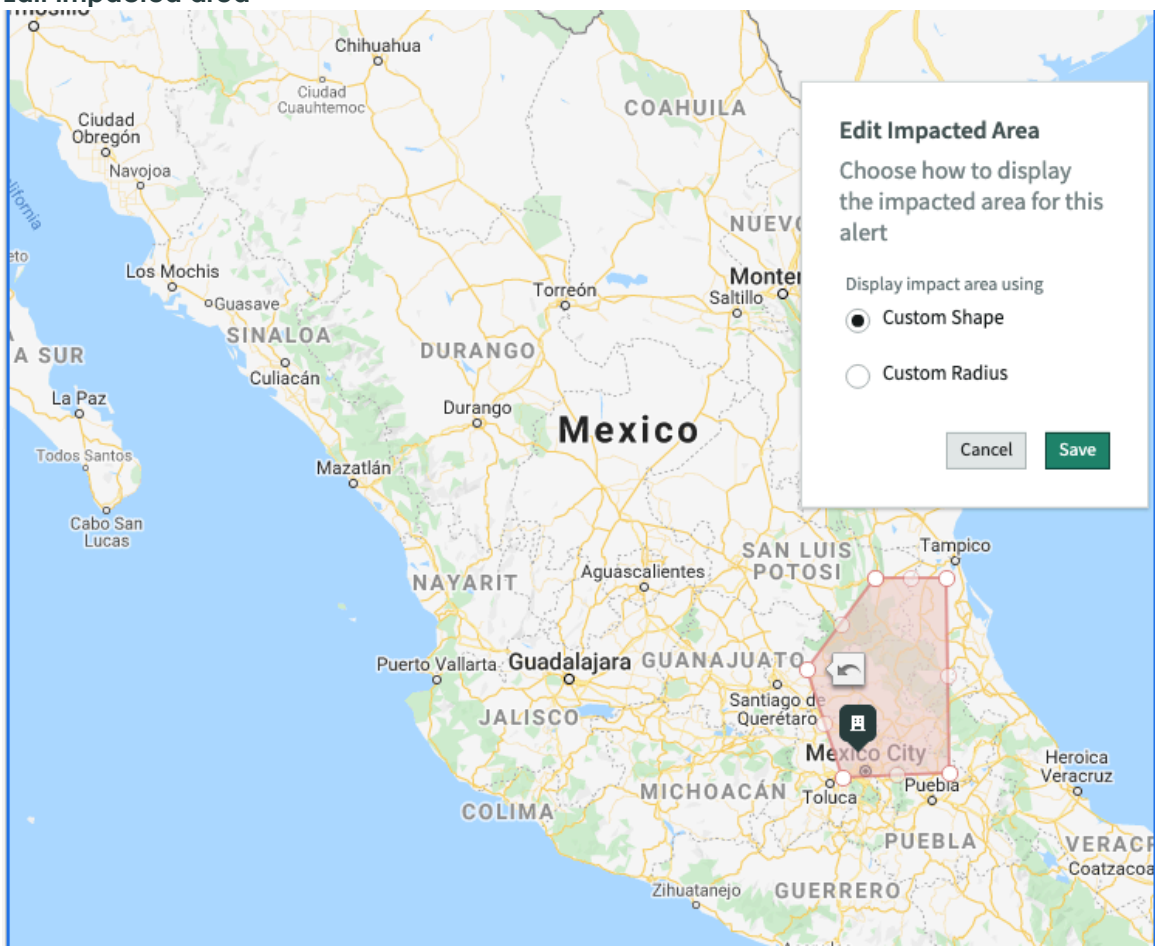
5. To edit an impacted area, click the alert menu icon ( ⋮ ).

   a. Click the **Edit Impact Area** option.

   b. In the Edit Impacted Area pop over that opens on the map, select either Custom Shape or Custom Radius depending on the shape of the impacted area.
      - Custom Shape: Select Custom Shape if the impacted area is polygonal shape.
      - Custom Radius: If the impacted area is a circle.

   c. Click and drag the vertex on the boundary of the impacted area to include the asset location.

**Edit impacted area**




   d. Click **Save**.

6. Save or bookmark the URL of the alert to open the detailed view of the alert directly anytime.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Click an asset card like a location or datacenter in the **Assets at Risk** section.
   The list view of the records opens up in a new tab.
8. To view the details of the asset, click the link to the record in the **Name** column.
   You can view the complete details of the asset including its latitude and longitude.

### Notify stakeholders and initiate Crisis Management response workflows

Notify the stakeholders and initiate multiple workflows for the recovery teams across your organization and help them respond to the threat and take necessary actions.

#### Before you begin

Role required: BCM admin or BCM Program Manager

#### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the map icon (  ).
3. Click an alert record.

   As a crisis manager, while viewing the alerts and their severity, you can initiate appropriate actions and trigger Crisis Management workflows for the respective stakeholders to respond and act on the crisis. The **Suggested Actions** section lists various responses that you can initiate.

   Notify Stakeholders

   Notify important stakeholders of the assets that are at risk because of the alert.

   Declare a Crisis Event

   Start an event to activate the recovery tasks to recover the assets with a recovery team.

4. To notify a stakeholder of the impending crisis by an email, click the **Notify** button in the Notify Stakeholders card.
   In the modal window that opens, identify the concerned person or persons and communicate the information to them. It is a two-step process, where you identify the audience and draft an email to send it to them.

   a. Select an audience from the list in the Notify Stakeholders pop-up.
      You can select an additional audience from the list whom you think must be notified too.

   b. Click **Next**.

   c. In the Step 2 of the process, verify the alert details and draft an email appropriately in the **Email Body** field.

   d. Click the **Send Notification** button.
      You get a message that the action is executed.

5. To activate a business continuity or disaster recovery plan for the locations that are impacted, click **Declare Crisis** in the Declare a Crisis Event card.
   a. Enter a brief description of the crisis event in the Declare a Crisis Event modal window that opens.
   b. Click **Next**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

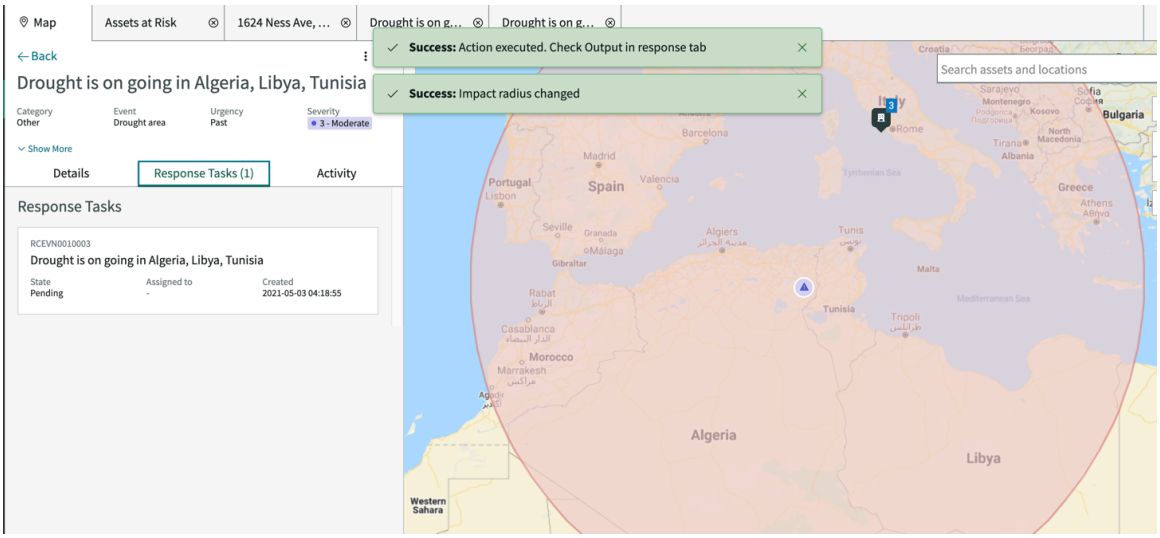
c. Select the assets at risk that are within the radius of the threat alert.

d. Click **Start Crisis Event** button.

When you trigger these actions, separate scripts run to trigger the alert notify action and the declaration of the crisis event. A message appears to confirm that your actions are executed. You can navigate to the **Response Tasks** tab to view the action and recovery event details.

All the assets at risk are copied over to the Event Assets table [sn_recovery_event_asset] related to the event [sn_recovery_event].

**Declare a crisis event**




## What to do next

1. If it is a recovery event, click anywhere on the Response Tasks card to take you to the event details.
2. In the **Details** tab of the event, update the details if required.
3. Click the **Start Event** button. The event for the crisis is then activated. All the associated plans for this recovery event and the tasks associated with it are set into action. The Crisis Management workflow begins to recover the impacted assets. For more information, see Manage a crisis event.

   All the assets at risk are copied over to the Event Assets table [sn_recovery_event_asset] related to the event [sn_recovery_event].

## Integrating Crisis Management with Everbridge notifications system

You can integrate Crisis Management in Business Continuity Management application with Everbridge notifications system. Everbridge system enables you to send emergency notification to individuals or group of people alerting them of an impending emergency. It provides a one-way notification and two-way communication through properly established delivery channels.

Crisis Management in Business Continuity Management application uses Everbridge to direct certain crisis response activities. This integration helps to send notifications about critical events to stakeholders and coordinates responses from them in an effective two-way delivery channel.

To send a notification, you need correct contacts, groups, and delivery channels. Delivery channels are created and stored in Everbridge and you have to import those delivery

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

channels for your particular organization ID. These delivery channels are used for sending notifications and contact creation.

### Setup steps for emergency notification

Setting up the Emergency Notification feature requires you, as a BCM admin, to configure certain pre-requisite data. The setup steps help you to establish a consistent connection with Everbridge and a successful notification delivery workflow on the Everbridge side.

The following configurations are required to be set up for different users to use the Crisis Management workspace for sending an emergency notification and monitoring the notification workflow:

- To create a connection and authenticate your credentials with Everbridge, seeCreate connection and authenticate credential with Everbridge.
- To get the delivery details of the contacts from Everbridge and use them to send notification, see Import delivery channels from Everbridge.
- To get the details about the type of contacts from Everbridge, see Import record types from Everbridge.
- To pre-configure a notification template to send an email or SMS to your contacts, see Define a template for emergency notification.
- To create contacts for sending the notification, see Create contacts for emergency notifications.
- To set up rules in filtering the contacts from the user table, see Create contact import rules.
- To create a group of contacts, see Create a notification contact group.

Here is a flow diagram that shows how the different setup steps are connected for the integration:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Emergency notification setup flow




## Create connection and authenticate credential with Everbridge

As a first step, establish a connection and authenticate your login credentials with an Everbridge instance to send out a notification using a delivery channel. This connection not only helps you to send but also receive communications.

### Before you begin

Role required: BCM admin (sn_bcm.admin)

### Procedure

1. Navigate to **Business Continuity** > **Everbridge Notification Configuration** > **Connection & Credential Alias**.
2. Click the **Create New Connection & Credential** related link.
3. On the form, fill in the fields.

#### Create Connection and Credential form

| Field | Description |
|---|---|
| Connection Name | Name of the connection. Enter Everbridge Connection. |
| Connection URL | Everbridge API base address. |
| Organization ID | Organization ID of Everbridge. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** You can get the organization ID from the Everbridge instance. |
| Incident Template ID | Unique ID of Everbridge incident template.<br>**Note:** You can get the ID from the Everbridge instance. |
| Credential Name | Name of Everbridge credential. |
| Username | User name of API user in Everbridge. |
| Password | Password to validate and establish connection. |

4. Click **Create**.

### Import delivery channels from Everbridge

After setting up the connection and credentials with Everbridge, you must import the delivery channels from Everbridge. Sending notifications is made easier through these delivery channels.

#### Before you begin
Role required: BCM admin (sn_bcm.admin)

#### About this task
Finding out how to reach or connect with your stakeholders at the time of crisis may have many challenges. Your notifications may not reach them as they may no longer use those delivery methods through which you are trying. Having imported delivery channels to reach your contacts and selected groups make your notification service much more certain and manageable.

#### Procedure
1. Navigate to **Business Continuity** > **Everbridge Notification Configuration** > **Delivery Channels**.
2. Click **Import**.
   All delivery channels are imported from Everbridge successfully. You get a message of confirmation if successful, otherwise an error message.

### Import record types from Everbridge

Import the record types for your organization ID from Everbridge and use them to create contacts.

#### Before you begin
Role required: BCM admin (sn_bcm.admin)

#### About this task
Record types are information stored in Everbridge which are required to create contacts.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **Business Continuity** > **Everbridge notification Configuration** > **Record Types**.
2. Click **Import**.
   Record types for your organization ID with the category are imported from Everbridge. If successfully imported you get a message of confirmation, otherwise an error message.

#### Define a template for emergency notification

Create a template with pre-defined information that you can use to send notification quickly to your users in an emergency.

### Before you begin
Role required: BCM admin (sn_bcm.admin)

### About this task
For example, you can define a template drafting an email information for a particular emergency crisis that might strike a business location or facility specifically.

### Procedure

1. Navigate to **Business Continuity** > **Everbridge Notification Configuration** > **Notification Templates**.
2. Click **New**.
3. On the form, fill in the fields.

**Notification Template form**

| Field | Description |
|---|---|
| Name | Name of the notification template. |
| Description | Short note about the purpose of the template. |
| Delivery channels | Communication channels used for sending the notification. |
| Subject | Title of the notification. |
| Message body | Introductory text message for the notification. |
| Foot note | Closing message for the notification. |
| SMS text | Message sent through SMS. |

4. Click **Submit**.

#### Create contacts for emergency notifications

Use the ServiceNow users list to create contacts manually and synchronize the contacts with Everbridge to send emergency notifications.

### Before you begin
Role required: BCM admin (sn_bcm.admin)

### About this task
After creating the contact from the user list, you can update the contacts and synchronize them with Everbridge.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Delivery channels are imported from Everbridge to the delivery channels table. Using the imported delivery channels, you can manually create contact delivery details or the system administrator can do an easy import.

### Procedure

1. Navigate to **Business Continuity** > **Everbridge Contact Configuration** > **Contacts**.
2. Click **New**.
3. On the form, fill in the fields.

**Contact form**

| Field | Description |
|---|---|
| Source | ◦ If you created the contact manually from the users list, then it is Manual.<br>◦ If you had used the sync rule to create contact, then it is Sync rule. |
| Last sync on | Auto-populates the date on which the contact was last synchronized with Everbridge. |
| Contact ID | Unique ID of the contact. |
| Sync status | Defaults to **New** when the contact is created. The status can also be:<br>◦ **Success**: When the contact is successfully synced with Everbridge.<br>◦ **Error**: If there is an error in syncing.<br>◦ **Updated**: If the contact or the delivery details were modified. |
| User | User reference from the Users table [sys_user]. |
| External contact ID | Contact ID in Everbridge. |
| Sync error | Error in syncing the contact with Everbridge. |

You can delete a contact that you created manually from the User table. However, the contact must be in **New** state. If the referenced user record is deleted, then a scheduled job that runs weekly deletes the contact from the Contacts table.

4. Click **Submit**.
5. To create delivery details for the contact you created, click **New** in the **Delivery details** related list.

   a. Select the Delivery channel from the list that you imported.

   b. Enter a value.
   If the delivery channel is email, then enter an email ID.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. Enter the order of preference in which the delivery channels are prioritized to send notifications.

d. Click **Submit**.

6. To import contacts using a sync rule, you must first create a contact import rule.
7. To import contacts based on contact sync rules, click **Import users** button.
   Refresh the form page to get the imported list of users.

   **Import users** action reads the Users table [sys_user] based on the contact sync rules and creates a record in the Contacts table.
8. To synchronize your list of contacts with that of Everbridge, click the **Sync with Everbridge** button.
   After the contacts are synchronized with Everbridge, the status of the sync action is recorded in the **Sync status** field. The unique ID of the contacts that are synced successfully in Everbridge are recorded as the **External contact ID** of the Contacts table.

### Create contact import rules

Create a contact import rule to apply on the User table and filter out users as contacts for emergency notifications.

#### Before you begin
Role required: BCM admin (sn_bcm.admin)

#### About this task
The contact import rule is applied on the default table that is the User table [sys_user]. The unique user reference that is the sys_id of the user table and the unique contact ID of the Contacts table that is synced with Everbridge are mapped.

#### Procedure
1. Navigate to **Business Continuity** > **Everbridge Contact Configuration** > **Contact Import Rules**.
2. Click **New**.
3. On the form, fill in the fields.

**Contact Import Rules form**

| Field | Description |
|---|---|
| Name | Name of the import rule. |
| Table | Defaults to the User table [sys_user] |
| Filter condition | Condition applied on the User table to filter records. |
| Record type | Default category of the record type. |
| User mapping | Unique user reference from the Users table. |
| Contact ID mapping | Unique ID of each contact used to sync with Everbridge. |

4. Click **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create a notification contact group

Create a notification contact group using the Now Platform groups. Use the group members as contacts for emergency notification. Synchronize the group members as contacts with Everbridge and track the non-synchronized members as exceptions.

#### Before you begin

Role required: BCM admin (sn_bcm.admin)

#### Procedure

1. Navigate to **Business Continuity** > **Everbridge Contact Configuration** > **Notification Contact Groups**.
2. Click **New**.
3. On the form, fill in the fields.

**Notification Contact Group form**

| Field | Description |
|---|---|
| Group | Reference to the User Group table. |
| Sync status | Defaults to **New** when the group is created.<br>◦ **Success**: The contact group is successfully synchronized with Everbridge.<br>◦ **Error**: If there is an error in syncing.<br>◦ **Updated**: If the contact group is modified. |
| Last sync on | Auto-populates the date on which the group was last synchronized with Everbridge. |

4. Click **Submit**.
5. To synchronize the group with the groups in Everbridge, click **Sync Groups to Everbridge**. Refresh the page to get the synchronized status of the group.

   If a group did not synchronize with Everbridge, then you get an error message.

6. To view the names of the group members that did not synchronize with Everbridge, click **Group User Exceptions** related list.

#### Example:

There are five members in a group, out of which four members are already synced with Everbridge and existing as contacts. When you synchronize the group, a group is created in Everbridge with the four synced group members. However, the unsynchronized single member is logged as an exception displaying a message as to why the syncing failed.

You can synchronize this particular contact first and then the group with Everbridge.

### Create an emergency notification and monitor its workflow in the workspace

Use the **Emergency notification** tab in the event workspace to create a notification for a crisis event or an exercise event where the exercise method is Functional.

#### Before you begin

Role required: sn_bcm.planner, sn_bcm.program_manager, or sn_bcm.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

Send an event notification from the workspace that triggers a complete workflow of activities from the **Draft** to **Complete** state in Everbridge, where all the activities can be monitored from the workspace.

When you send an emergency notification from the workspace, the action creates an incident and a notification for the incident in Everbridge to be sent to the right contacts and groups.

### Procedure

1. Navigate to **Business Continuity** > **Business Continuity Workspace**.
2. Click the lists icon (  ).
3. Click **Pending** state in the Crisis Events list.

   **Note:** If the **Exercise Method** is **Functional**, then you can create an emergency notification for an exercise event.

4. Click the link to the event record in the **Number** column.
5. Click the **Emergency Notifications** related list.
6. Click **New**.
   New Notification form opens in a separate tab.
7. On the form, fill in the fields.

**Create New Notification form**

| Field | Description |
|---|---|
| Short description | Title of the emergency notification |
| Template | Pre-configured template that has the subject of the mail and the delivery channels for the contacts. |
| Notification state | State of notification in the ServiceNow workspace. |
| Communication status | State of notification in Everbridge. |
| Description | Description of the notification. |
| Contacts and Groups | |
| Contacts | Persons to whom the notification is sent.<br><br>Contacts that are successfully synced with Everbridge are listed. |
| Notification contact groups | Groups of contact to whom the notification is sent.<br><br>Successfully synced contact groups are listed. |
| Settings | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Acknowledgement required | Option if an acknowledgement is required from the contact for the notification received. |
| Delivery channels | Communication channels used for sending the notification. |
| Message Details | |
| Subject | Title of the notification. |
| Message body | Introductory text message for the notification.<br><br>If a template is selected, then the message details are auto-populated from the template. |
| Foot note | Closing message for the notification. |
| SMS text | Message sent through SMS. |

The notification that you create is in **Draft** stage.

8. To save the notification and send it later, click **Save**.
9. To delete the notification that is in **Draft** stage, click **Delete**.
10. Click **Send**.

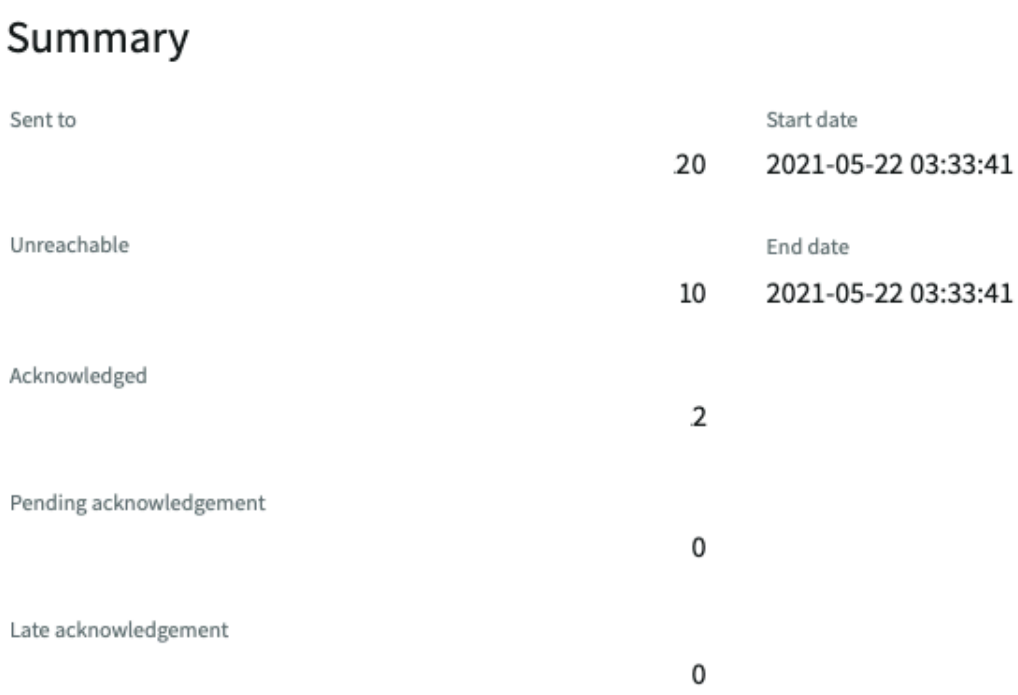
    The send action creates a notification in Everbridge.

    When you create and send a notification for a crisis event in the workspace, a corresponding incident is created along with a notification in Everbridge.

11. To know if there are any errors in sending the notification, refresh the page.
    If there is an error in sending, the **Notification state** moves to **Error**.
12. To get the state from Everbridge for the notification sent to the contacts in the **Communication status** field, click the **Get response status** button.
    The **Summary** section displays the list of contacts and groups to whom the notification was sent and their responses. It also displays the number of contacts who could not be reached, the number of contacts who acknowledged the notification, and the number of pending acknowledgements. This information is retrieved from Everbridge and displayed on your workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Summary of the notification sent to contacts**




Sent to
: Number of contacts to whom the notification was sent.

Unreachable
: Number of contacts to whom notification was not sent.

Acknowledged
: Number of contacts who acknowledged the receipt of notification.

Pending acknowledgement
: Number of contacts who did not acknowledge the receipt of notification.

Late acknowledgement
: Number of contacts who confirmed the receipt of notification after the notification duration had elapsed.

If there are many contacts to whom the notification could not be delivered, then create another notification for the same crisis event. This time, you can send to a team of managers, as the previous notification did not reach many contacts.

Before you submit an event for approval, all the notifications that are In Progress must be closed.

**a.** To delete a notification that is in **Draft** or **Error** state, click the link to the emergency notification record in the **Number** column.

> **Note:** You cannot delete a notification that is in **Attempting to send**, **In Progress** or **Completed** state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**b.** Click **Delete** in the more actions icon ( ).

**Note:** Now that the event is closed and the corresponding incident in Everbridge is also closed, you cannot create any more notifications for this event.

#### Workflow status of the emergency notification

The table lists the different states to which the emergency notification proceeds in the Everbridge side. You can track the notification delivery and monitor its status in the workspace until it is successfully delivered to the contacts from the Everbridge side.

### Status flow of emergency notification

An emergency notification that you create for a crisis event, when sent to Everbridge creates a corresponding incident along with a notification. The short description of the event in the workspace is created as an incident with a notification in Everbridge.

Notification state

The emergency notification that is created and sent from ServiceNow Business Continuity Management workspace is tracked in the **Notification state** field.

Communication status

The emergency notification that is received in Everbridge and the different stages to which it moves until it is delivered are tracked in the **Communication status** field.

#### Emergency notification workflow status

| Notification state | Communication status |
|---|---|
| **Draft**: Draft is stored in the workspace. | |
| **Attempting to send**: Notification is being sent from the workspace. | |
| **Error**: Error in creating the notification in Everbridge. | |
| **In Progress**: Notification is successfully created in Everbridge. | **Active**: A notification is created and is active.<br><br>An incident and a notification for the incident are created. The notification remains active for the duration set in Everbridge. |
| | **Sent**: After the set duration has elapsed, the state moves to Sent. |
| **Completed**: The notification is sent. | |
| | **Stopped**: Notification is stopped from being sent. |

## Business Continuity Management reference

Reference topics provide additional information such as tables, roles, and properties that are installed with the Business Continuity Management application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Components installed with Business Continuity Management

Several types of components are installed with activation of the Business Continuity Management application.

### Roles installed

| Role title [name] | Description | Contains roles | Available with scope |
|---|---|---|---|
| BCM administrator<br><br>[sn_bcm.admin] | Create, read, write, and delete access to all tables including the core data. | • sn_bcm.program_manager<br>• sn_bcm.core_manager<br>• sn_bia.bia_admin<br>• sn_bcp.plan_admin<br>• sn_grc_appr.admin<br><br>**Note:**<br><br>The BCM admin contains the Approver Configurator admin role, but it doesn't contain the Approver Configurator developer role.<br><br>For security reasons, the Approver Configurator admin has read access to the **Script** field on the Approval Rule form. If you have the Approver Configurator developer role in the GRC: Approver Configurator application, you've create and write access to the **Script** field on the Approval Rule form.<br><br>For more information on the roles in the GRC: Approver Configurator application, see Roles installed with GRC: Approver Configurator. | Business Continuity Management – Core |
| BCM Program Manager<br><br>[sn_bcm.program_manager] | Create, read, write, and delete access to all | • sn_bcp.plan_manager<br>• sn_bia.bia_manager | Business Continuity |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role title [name] | Description | Contains roles | Available with scope |
|---|---|---|---|
| | BCM application tables. | • sn_recovery.event_manager<br>• sn_bcm.core_viewer<br>• workspace_user<br>• service_viewer | Management – Core |
| BCM Planner<br><br>[sn_bcm.planner] | Create, read, write, and delete access to all BCPs, BIAs, exercises, and crisis events that are created or owned by the planner.<br><br>**Note:** If you have the BCM planner role and you are not the owner of the exercise, you cannot remove the assets from an exercise or remove a plan from the exercise, but you can add the assets or a plan. Additionally, if you are not the plan owner, you can only add the approved plans in an exercise or crisis event. | • sn_bia.bia_planner<br>• sn_bia.bia_viewer<br>• sn_bcp.plan_contributor<br>• sn_recovery.event_user<br>• sn_bcm.core_viewer<br>• workspace_user<br>• service_viewer | Business Continuity Management – Core |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role title [name] | Description | Contains roles | Available with scope |
|---|---|---|---|
| BCM Contributor [sn_bcm.contributor] | • Read access to all BIAs, exercises, and crisis events tables.<br>• Read access to BCP tables if the contributor is included in the contributor list.<br>• Create and delete existing dependencies when the group is in pending state.<br>• Write access to the RTO, RPO, and dependency category state fields, disruptive duration of RTO and RPO editable fields, and dependency assessment editable fields.<br>• Update RTO, RPO, and dependency assessment state. | • sn_bia.bia_contributor<br>• service_viewer<br>• sn_bcm.core_viewer | Business Continuity Management – Core |
| BCM Viewer<br><br>[sn_bcm.viewer] | View all data of the BCM applications. | • sn_recovery.event_viewer<br>• workspace_user<br>• sn_bia.bia_viewer<br>• sn_bcp.plan_viewer<br>• service_viewer<br>• sn_bcm.core_viewer | Business Continuity Management – Core |
| BCM Recovery Team member [sn_bcm.recovery_team_member] | View the list of recovery tasks for crisis events and exercises | • sn_recovery.event_viewer<br>• sn_bcp.plan_viewer | Business Continuity Management – Core |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role title [name] | Description | Contains roles | Available with scope |
|---|---|---|---|
| | assigned by the BCM Program Manager. | • sn_bcm.core_viewer<br>• sn_recovery.event_member | |
| Approval configuration admin [sn_grc_appr.admin] | Create, read, write, and delete access to all approver configurator setup tables. | **Note:** To approve an approval configuration record in the BCM application, you must have a BCM role. If you add a user with a non-BCM role to the approval process of an approval configuration record, the record may become inaccessible due to being in an inaccessible state. | Business Continuity Management – Approver Configurator |
| Approver [sn_grc_appr.approver] | Create, read, write, and delete access to the Approval table. | | Business Continuity Management – Approver Configurator |

## BCM lite operator role

For information on the BCM lite operator role, see Business Continuity Management lite operators.

## Tables installed

| Table | Description | Installed with scope |
|---|---|---|
| BCM Choice [sn_bcm_choice] | For the BCM admin to configure choice options in BCM applications. | Business Continuity Management – Core |
| Documentation Section [sn_bcm_document] | Stores sections of a document for a plan. | Business Continuity Management – Core |
| Element Definition [sn_bcm_element_definition] | Stores all data for activity definitions. | Business Continuity Management – Core |
| Element variable [sn_bcm_element_variable] | Stores custom columns configured for an element definition. | Business Continuity |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Table | Description | Installed with scope |
|---|---|---|
| | | Management – Core |
| Grid configuration [sn_bcm_grid_configuration] | Stores configuration for a particular grid. For example, the dependency assessment grid. Grid configuration can have multiple grid column configurations. | Business Continuity Management – Core |
| Grid column configuration [sn_bcm_grid_column_configuration] | Stores data for columns that should be displayed for a grid configuration. | Business Continuity Management – Core |
| Impact analysis question [sn_bcm_impact_analysis_question] | Stores impact analysis questions for an impact category. | Business Continuity Management – Core |
| Impact Category<br><br>[sn_bcm_impact_category] | Stores the applicable timeframes and the maximum RTO value of a BIA. | Business Continuity Management – Core |
| Impact Rating<br><br>[sn_bcm_impact_rating] | Stores the impact ratings for an impact category. | Business Continuity Management – Core |
| Loss Scenario<br><br>[sn_bcm_loss_scenario] | Stores the elements impacted in a loss scenario. | Business Continuity Management – Core |
| Recovery Tier<br><br>[sn_bcm_recovery_tier] | Stores recovery timeframes applicable for a recovery tier level. | Business Continuity Management – Core |
| Recovery Timeframe<br><br>[sn_bcm_timeframe] | Stores the time duration at which a recovery timeframe starts. | Business Continuity Management – Core |
| Recovery Tasks<br><br>[sn_bcp_recovery_task] | Stores the activity tasks of all business continuity and recovery plans. | Business Continuity Management – Planning |
| Related Plan [sn_bcp_plan_plan] | Stores related plans for the primary plan in BCP. | Business Continuity Management – Planning |
| Plan Documentation | Stores the contents of a documentation section | Business Continuity |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Table | Description | Installed with scope |
|---|---|---|
| [sn_bcp_document] | that is a part of a plan template. | Management – Planning |
| Plan<br>[sn_bcp_plan] | Stores the status of business continuity and recovery plans. | Business Continuity Management – Planning |
| Plan Assets<br>[sn_bcp_plan_asset] | Stores the RPO, RTO, RTA, and RTO gap of the plan assets of all plans. | Business Continuity Management – Planning |
| Related Asset Dependency<br>[sn_bcp_plan_asset_dependency] | Stores the assets as configuration items that are dependent on a plan loss scenario. | Business Continuity Management – Planning |
| Plan Loss Scenario<br>[sn_bcp_plan_loss_scenario] | Stores the relationship between a plan and a loss scenario. | Business Continuity Management – Planning |
| Plan Task<br>[sn_bcp_plan_task] | Stores the configuration items identified for a plan task. | Business Continuity Management – Planning |
| Recovery Strategy<br>[sn_bcp_recovery_strategy] | Stores the recovery strategy associated to an asset identified in a plan loss scenario. | Business Continuity Management – Planning |
| Recovery Team<br>[sn_bcp_recovery_team] | Stores the users and groups assigned to the recovery team of a plan. | Business Continuity Management – Planning |
| Plan Template<br>[sn_bcp_template] | Stores the document sections, element definitions, and loss scenarios identified for each plan template. | Business Continuity Management – Planning |
| Dependency report source [sn_bia_dependency_report_source] | Stores columns that are tracked in a report. Used while creating an ad-hoc report on the dependency table. | Business Continuity Management – Impact Analysis |
| Impact Analysis<br>[sn_bia_analysis] | Stores all data related to BIA and the template is uses. | Business Continuity Management – Impact Analysis |
| Impact Category Result<br>[sn_bia_category_result] | Stores the impact category results of all BIAs. | Business Continuity Management |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Table | Description | Installed with scope |
|---|---|---|
| | | – Impact Analysis |
| Dependency<br><br>[sn_bia_dependency] | Stores the dependency groups and their item details. | Business Continuity Management – Impact Analysis |
| Impact Dependency Group<br><br>[sn_bia_dependency_group] | Stores element definitions or the dependency groups associated to a BIA. | Business Continuity Management – Impact Analysis |
| Result<br><br>[sn_bia_result] | Stores the category result, disruption duration, and the impact rating data. | Business Continuity Management – Impact Analysis |
| BIA Template<br><br>[sn_bia_template] | Stores the impact categories and dependency groups that a business process depends on. | Business Continuity Management – Impact Analysis |
| Score timeframe mapping [sn_bia_score_timeframe_mapping] | Stores the mapping results of the threshold score and the timeframe. | Business Continuity Management – Impact Analysis |
| Activated Plan<br><br>[sn_recovery_activated_plan] | Stores the list of recovery plans activated in an exercise or actual event. | Business Continuity Management – Recovery Exercise Management |
| Event<br><br>[sn_recovery_event] | Stores the status and owner details of events. | Business Continuity Management – Recovery Exercise Management |
| Event Assets [sn_recovery_event_asset] | Stores the asset name and the state whether the asset is recovered or not in an actual or exercise event. | Business Continuity Management – Recovery Exercise Management |
| Event Task<br><br>[sn_recovery_event_task] | Stores the status details and assignees of event tasks. | Business Continuity Management – Recovery |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Table | Description | Installed with scope |
|---|---|---|
| | | Exercise Management |
| Impacted Asset to Activated Plan [sn_recovery_impacted_asset_to_activated_plan] | Maps impacted assets with the activated plans. | Business Continuity Management – Recovery Exercise Management |
| Approval [sn_recovery_approval] | Store approval details of the event. | Business Continuity Management – Recovery Exercise Management |
| Approval Configuration [sn_grc_appr_approval_configuration] | Stores approval configuration information that applies to any business document like BIA, BCP, events, or any table. | Business Continuity Management – Approver Configurator |
| Approval Level [sn_grc_appr_approval_level] | Stores approval level information for an approval configuration of a business document. | Business Continuity Management – Approver Configurator |
| Approval Rule [sn_grc_appr_approval_rule] | Stores information of the approval rule applied to the business document. | Business Continuity Management – Approver Configurator |
| Approval [sn_grc_appr_approval] | Stores information of the approvers for each approval level. | Business Continuity Management – Approver Configurator |
| Approval [sn_bia_approval] | Stores information of the BIA approvers for each approval level. | Business Continuity Management – Impact Analysis |
| Approval [sn_bcp_approval] | Stores information of the BCP approvers for each approval level. | Business Continuity Management – Planning |

## Properties installed

For information on the properties installed with the Business Continuity Management application, see Properties installed with Business Continuity Management.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Script includes in Business Continuity Management

When you download the Business Continuity Management application, several scripts includes are added to your instance.

## Script includes updated for the Utah release

### Script includes updated for the Utah release

| Script-includes | Description |
|---|---|
| ActivePlanCandidateFilter | Contains the utility functions that are used in the BCP active plan filter. |
| BCPConstants | Contains the utility functions that are used in the BCP constants. |
| BCPDataVisualizationUtilsBase | Contains the utility functions that are used in the BCP data visualization. |
| BCPDependencySnapshotUpdateStrategyBase | Contains the API for updating the dependencies in plans. |
| BCPDocumentationRecordAPIBase | Contains the utility functions that are used in the BCP documentation record API base. |
| BCPDocumentationRecordAPI | Contains the utility functions that are used in the BCP documentation record APIs. |
| BCPRecordUI | Contains the utility functions that are used in the BCP record UI pages. |
| BCPRecordUIBase | Contains the utility functions that are used in the BCP record UI base. |
| BCPRecordAPI | Contains the utility functions that are used in the BCP record API. |
| BCPTemplateUtilsBase | Contains the utility functions that are used in the BCP template utilities base. |
| BIADependencySnapshotUpdateStrategyBase | Contains the API for updating the dependencies in the BIAs. |
| DependencySnapshotUpdateStrategyBase | Contains the API for the Update dependencies action and scheduled job. |
| EventDependencyUpdateStrategyBase | Contains the API for updating the dependencies in the events. |
| PlanRestAPIResourceUtil | Contains the utility functions that are used in the BCP Plan Rest API resource utility. |
| PlanRestAPIResourceUtil | Contains the utility functions that are used in the BCP plan Rest API resource utility. |
| PopulateBIAForPlanAsset | Contains the utility functions that are used to populate the BIA for the plan and asset. |
| PlanCopyUtilBase | Contains the utility functions that are used in the BCP plan copy utility base. |
| PlanUtil | Contains the utility functions that are used in the BCP plan utility. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Script includes updated for the Utah release (continued)**

| Script-includes | Description |
|---|---|
| PlanCommonUtils | Contains the utility functions that are used in the plan common utility. |
| RecoveryTasksUtil | Contains the utility functions that are used in the BCP recovery tasks utility. |

## Data Relationships Framework

The Data Relationships Framework application (sn_grc_rel_config) supports the BCM application with the underlying framework to fetch the dependencies in the BIAs, plans, and events from different sources such as CMDB, BIA, and BCP. Beginning with the Utah release, the Data Relationships Framework (sn_grc_rel_config) application is installed with the BCM application by default.

## Framework for fetching the dependencies

The Data Relationships Framework (sn_grc_rel_config) stores the configurations for how a main object type can relate to other object types. It enables the users to configure the source (main node) for the dependency updates, configure its relationship with the child nodes, and fetch the dependencies for the selected object.

A scheduled job scans the object configuration data at regular intervals and checks if any dependencies have been updated. If any changes are observed in the dependencies, the scheduled job fetches the dependencies of the selected object from one of the configured sources such as BIA, BCP, or CMDB.

## Benefits of the Data Relationships Framework

The Data Relationships Framework provides the following benefits for the BCM application users:

- Provides a single API to fetch the dependencies from different sources.
- Supports the configuration of the main node (source) and maintains its relationships with its child nodes such as assets, risks, and so on.
- Enables the users to control the performance by selecting different sources.

## Roles associated with the Data Relationships Framework

The following roles are associated with the Data Relationships Framework application.

**Roles associated with the Data Relationships Framework**

| Roles | Description |
|---|---|
| Data Relationships Framework administrator [sn_grc_rel_config.admin] | Configures the relationship of the object types such as the relationship of the main node to the child nodes. |
| Data Relationships Framework reader [sn_grc_rel_config.reader] | Views the data for the object types as defined in the Data Relationships Framework. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles associated with the Data Relationships Framework (continued)**

| Roles | Description |
|---|---|
| | **Note:** All BCM application users have the Data Relationships Framework reader role. |

## Tables for the framework

To support the Data Relationships Framework, the following new tables have been added and existing tables have been revised.

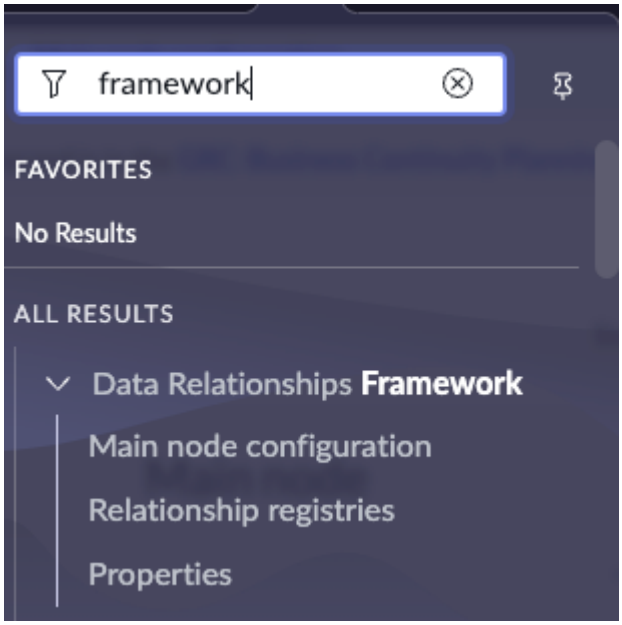
**Tables used for the Data Relationships Framework**

| New and existing tables | Table | Description |
|---|---|---|
| New table | Main node configuration [sn_grc_rel_config_main_node_config] | Table to store the configuration of the main node from where the dependencies are fetched. |
| New table | Node relationship configuration [sn_grc_rel_config_node_rel_config] | Table to store the configuration that determines the dependencies of the main node and child nodes. It also maintains a reference to the main node configuration. |
| Existing table | Relationship registries [sn_data_registry_relationship] | Table to determine the relationship of an object with other objects. |

## Modules for configuring the relationships

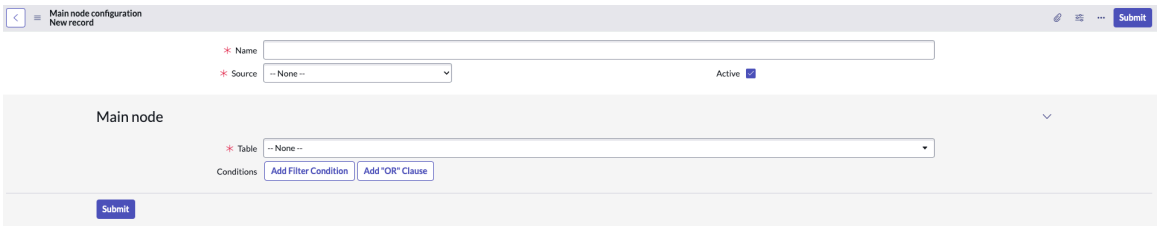
The BCM application users can navigate to **Data Relationship Framework** in the application navigator and access its modules for configuring the relationships.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

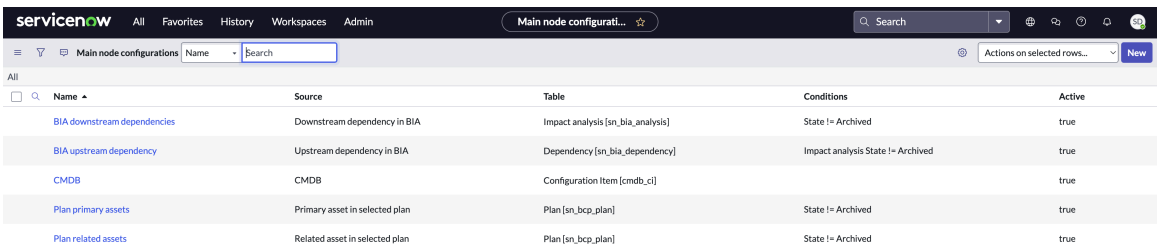



The Data Relationships Framework application consists of the following modules:

1. Main node configuration: Configure the details of the main node such as its name, source, table name, filer conditions, and so on as shown in the following examples.




The following main node configurations are provided as sources with the base system as shown in the following example:

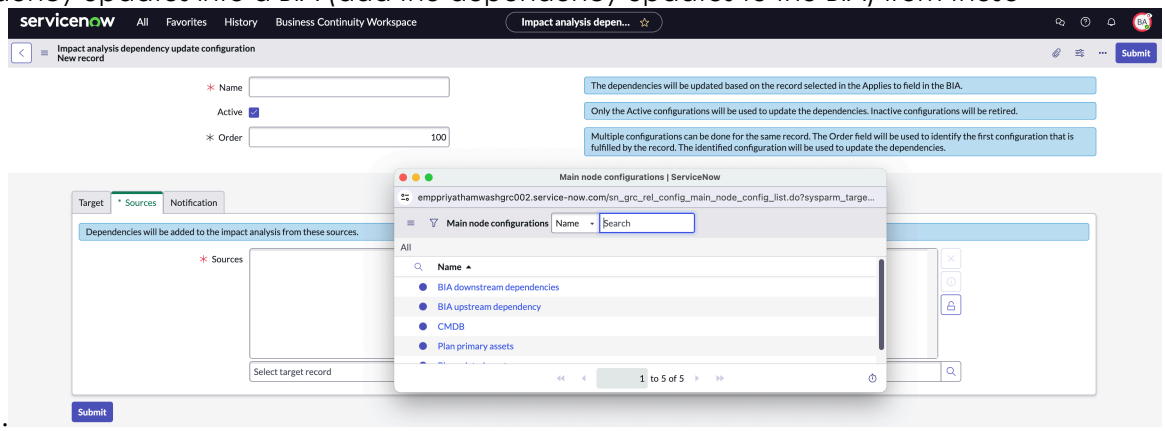



- BIA upstream dependency
- BIA downstream dependencies
- CMDB
- Plan primary assets
- Plan related assets

The BCM administrators use the main node configuration to perform the following tasks:

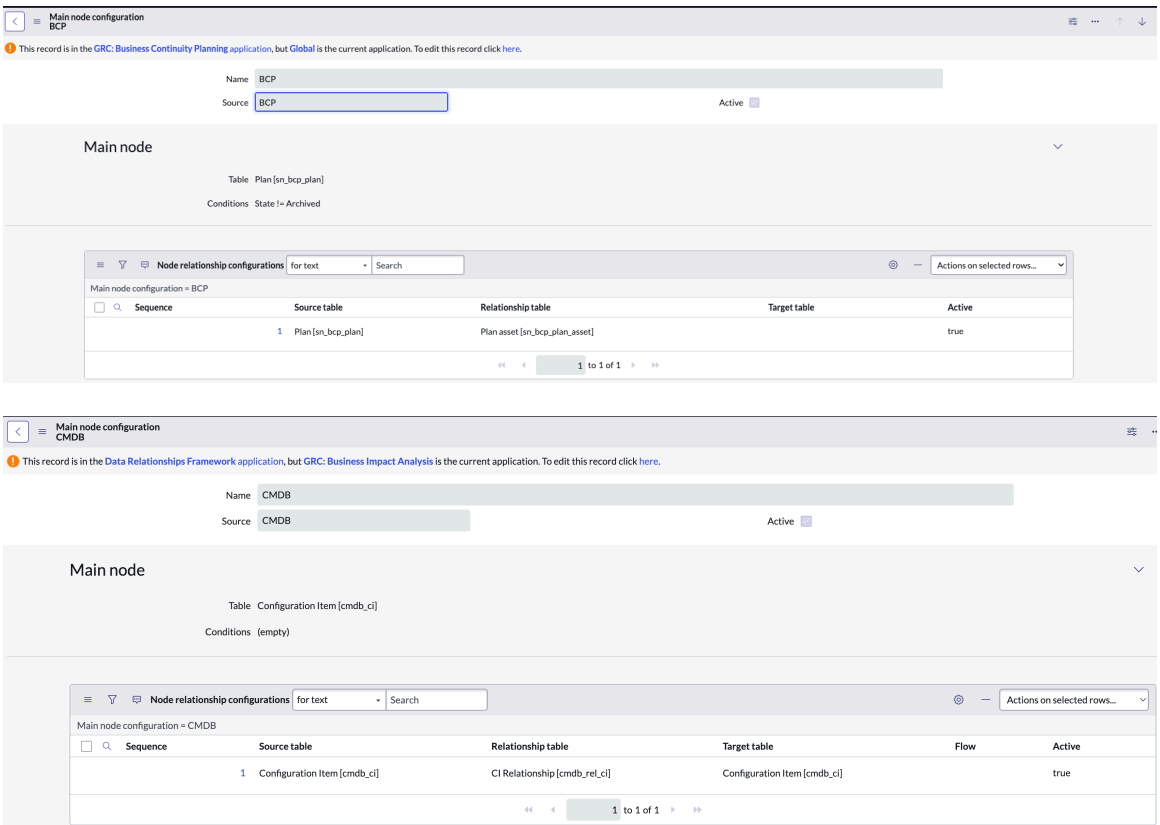
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Configure the Impact analysis dependency update configuration module and fetch the dependency updates into a BIA (add the dependency updates to the BIA) from these sources.




- Configure the Planning dependency update configuration module and fetch the planning dependency updates into a plan (add the updated related assets to the plan) from these sources.
- Configure the Event dependency source configuration module and configure the sources for the event dependency updates (add the updated impacted assets to a recovery event).

The main node configuration records for plans and CMDB are shown in the following examples.

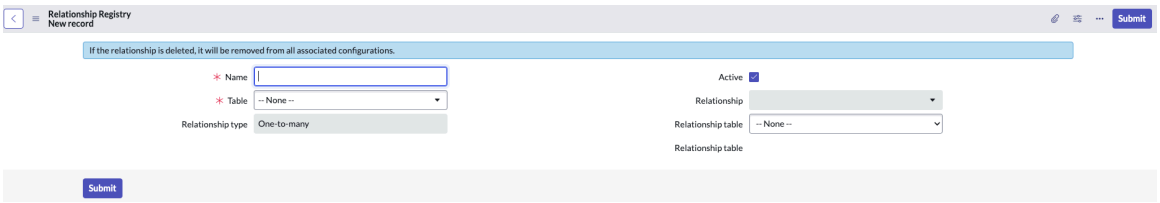



For information on creating a main node configuration record, see Create a main node configuration record.

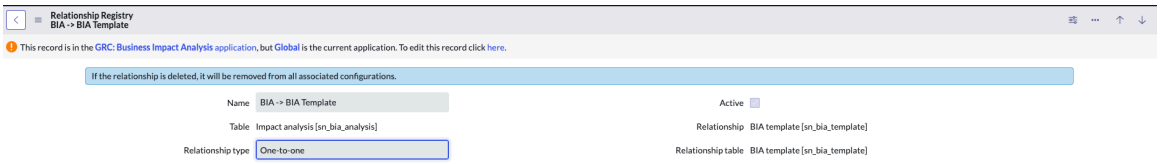
2. Relationship registries: Configure the relationship registries for the main node. Relationship registries are part of the 360-degree configuration in GRC where a user can define how

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

one object has a related object. The configuration details of a relationship registry record such as its name, table, relationship type, relationship table, and so on are shown in the form.

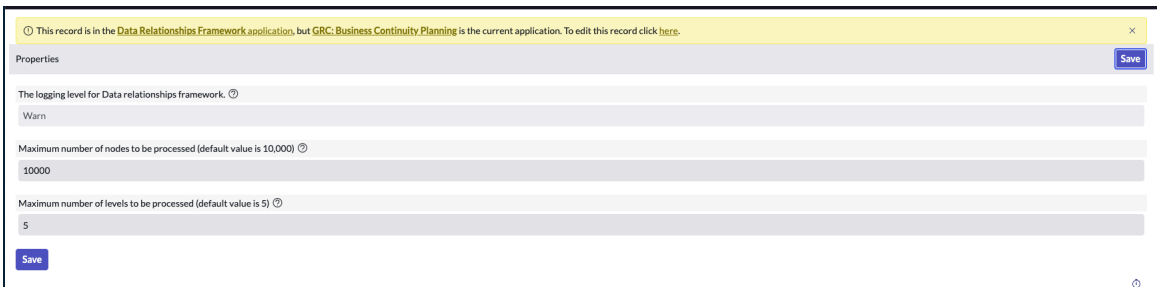



A sample relationship registry record for a BIA and BIA template is shown in the following example.




For information on creating a relationship registry record, see Create a relationship registry record.

3. Properties: Configure the properties of the Data Relationships Framework as shown in the following example.



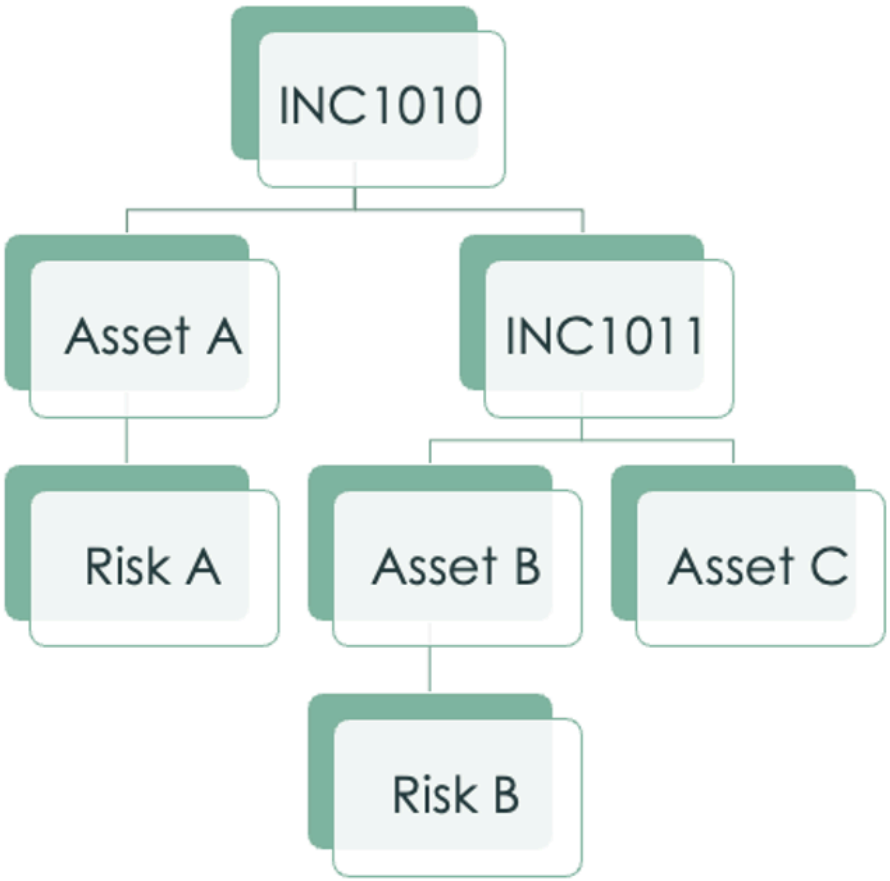

For information on configuring the properties, see Configure the properties for the Data Relationships Framework.

## Use cases for the Data Relationships Framework

The Data Relationships Framework is used to configure the node and asset relationships such as mapping a main node to its child node or mapping an asset to a risk.

Consider the following use case that shows the main node configuration and its relationships.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




In this example, INC1010 is the main node where the source is an Incident. INC1010 has two child nodes:

1. Asset A: The affected configuration item for Asset A is Risk A.
2. INC1011: The affected configuration items (CIs) for INC1011 are Asset B and Asset C. For Asset B, the affected configuration item is Risk B.

With the underlying Data Relationships Framework, the following relationships are configured:

- Main nodes:
  - INC1010 -> Asset A
  - INC1010 -> INC1011
- Node relationships:
  - Asset A -> Risk A
  - INC1011 -> Asset B
  - INC1011 -> Asset C
  - Asset B -> Risk B
- Input nodes:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Source = Incident
- Record = INC1010
- Max Levels = 5
- Max Nodes = 1000

- Output nodes:
  - INC1010
  - Asset A
  - INC1011
  - Risk A
  - Asset B
  - Asset C
  - Risk B
- Edges:
  - INC1010 -> Asset A
  - INC1010 -> INC1011
  - Asset A -> Risk A
  - INC1011 -> Asset B
  - INC1011 -> Asset C
  - Asset B -> Risk B

## Limitations of using the Data Relationships Framework

The Data Relationships Framework has the following limitations:

- The data fetched for an object cannot be reused for another purpose.
- The sources provided in the framework must be used for fetching the dependency updates into an object. It is not possible to configure your own sources for fetching the data.

### Create a main node configuration record

Create a main node configuration record to configure the source for fetching the dependencies. You can configure the details of the main node such as its name, source, table name, filer conditions, and so on.

#### Before you begin

Role required: sn_grc_rel_config.admin

#### Procedure

1. Navigate to **All** > **Data Relationships Framework** > **Main node configuration**.
2. Select **New**.
3. On the form, fill in the fields.
   For information on the fields in the form, see Main node configuration new record form.
4. Select **Submit**.
   The main node configuration record is displayed in the Main node configurations list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Main node configuration new record form

Use the Main node configuration new record form to create a main node configuration record in the Data Relationships Framework.

## Main node configuration new record form

**Main node configuration new record form**

| Field | Description |
|---|---|
| Name | Name of the main node configuration record. For example, BCP. |
| Source | Source for the main node configuration record. Available options are:<br>• **BIA upstream dependency**<br>• **BIA downstream dependencies**<br>• **CMDB**<br>• **Plan primary assets**<br>• **Plan related assets** |
| Active | Option to indicate that the record is active. |
| Table | Table used to set up the relationship. For example, Plan [sn_bcp_plan]. |
| Condition | Filter condition used to set up the relationship for the configuration record. For example, you can set the condition as *"Status in source" "is" "Valid"*. |

### Create a relationship registry record

Create a relationship registry record to set up relationship between the record and object defined in the table. You can configure the details of the main node such as its name, source, table name, filer conditions, and so on.

### Before you begin

Role required: sn_grc_rel_config.admin

### Procedure

1. Navigate to **All** > **Data Relationships Framework** > **Relationship registries**.
2. Select **New**.
3. On the form, fill in the fields.
   For information on the fields in the form, see Relationship registry new record form.
4. Select **Submit**.
   The relationship registry record is displayed in the Relationship Registries list.

### Relationship registry new record form

Use the Relationship registry record form to create a relationship registry record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Relationship registry new record form

### Relationship registry new record form

| Field | Description |
|---|---|
| Name | Name of the relationship registry record. For example, BIA analysis –> Issue. |
| Table | Table used to set up the relationship registry record. For example, Impact analysis [sn_bia_analysis]. |
| Relationship type | Relationship type for the relationship registry record. Available options are:<br>• **One-to-one**: One record has a relationship to one record in another table.<br>• **One-to-many**: One record has a relationship to one or more records in another table.<br>• **Many-to-many**: One or more records have a relationship to one or more records in another table.<br>• **Scripted relationship**: Use scripts to define the relationship between the tables. |
| Active | Option to indicate that the relationship registry record is active. |
| Relationship | Table used to set up the relationship with the object that is defined in the **Table** field. For example, Issue [sn_grc_issue]. |
| Relationship table | Read-only field. The table selected in the **Relationship** field is displayed as a relationship table by default. For example, Issue [sn_grc_issue]. |

### Configure the properties for the Data Relationships Framework

Configure the properties for the Data Relationships Framework application.

#### Before you begin

Role required: sn_grc_rel_config.admin

#### Procedure

1. Navigate to **All** > **Data Relationships Framework** > **Properties**.
2. Update the properties in the form.
   For information on the properties in the form, see Data Relationships Framework properties form.
3. Select **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Data Relationships Framework properties form

Use the Data Relationships Framework properties form to configure the relationship properties for Data Relationships Framework APIs.

## Data Relationships Framework properties form

**Data Relationships Framework properties form**

| Field | Description |
|---|---|
| The logging level for Data Relationships Framework | Logging level for the Data Relationships Framework. Available options are:<br>• **Debug**<br>• **Info**<br>• **Warn**<br>• **Error**<br>The default value is Warn. |
| Maximum number of nodes to be processed | Maximum number of nodes to be processed when the Data Relationships Framework API is called.<br>The default value is 10,000. For example, when the API is called, it displays the results for a maximum 10,000 nodes. |
| Maximum number of levels to be processed | Maximum number of levels to be processed when the Data Relationships Framework API is called.<br>The default value is 5. For example, when the API is called, it processes maximum 5 levels of the relationships and does not go deeper than 5 levels. |

## Domain separation and Business Continuity Management

Domain separation is supported for Business Continuity Management. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

## Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

For more information on support levels, see Application support for domain separation.

## Overview

Business Continuity Management supports domain separation. The tables are striped with the domain ID and domain path. Domain separation for Business Continuity Management means that only a user in the application's domain or parent domain can access the data. All functionality for Business Continuity Management works in a domain-separated environment as long as the Business Continuity Management actions are performed by users within that domain.

## How domain separation works in Business Continuity Management

Domain separation is supported only at the data level for Business Continuity Management. Cross-level scheduled job data setup is not supported. Therefore, you must copy the scheduled job in each of your domain to respect the data level separation.

To set up domain separation for Business Continuity Management:

1. Create your domain and then create Business Continuity Management users in that domain.
2. Only a specified user (Business Continuity Management admin in that domain) should populate configuration data in the domain of the application.
3. Only users in the application's domain should upload or create data in the domain.

Follow these guidelines for successful domain separation:

- Create a separate user for each domain to perform upload, edit, or export of configuration data.
- Avoid uploading or creating configuration data for a given application in multiple domains.
- Only users in the application's domain should upload or create data in the domain.
- Policies and exporters must be either in the application's domain or in the global domain.

## Domain-separated tables in Business Continuity Management

All Business Continuity Management tables include a **Domain** column.

Related topics

Domain separation for service providers

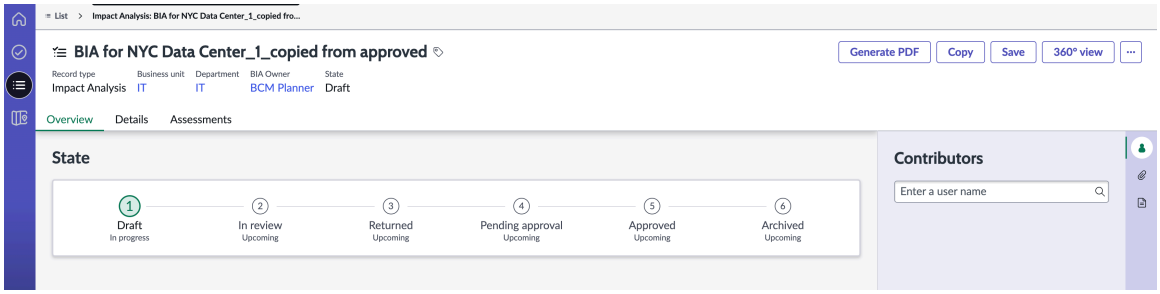
## GRC record page template for BCM records

Beginning with the Utah release, the GRC records use the common GRC record page template. You can leverage the new variant of record pages to streamline page creation, simplify maintenance, and minimize the cost of page ownership.

With standard record page migration, you can configure consistent styling and a uniform look for all BCM records. You can also configure the header of the record to display additional information such as priority, due date, issue source, issue type, and so on.

A record in the BCM application with the GRC record template is shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**Note:** If you are upgrading to the version 17.x apps, you can also revert to the previous record page.

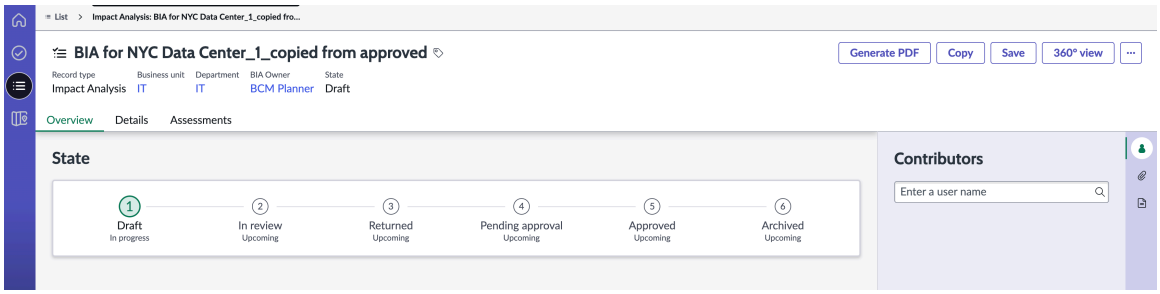
### Stepper component in the Overview tab of the records

The stepper component on the **Overview** tab shows the progression of the states for the record.

### Stepper component in the Overview tab of the records

The stepper component on the **Overview** tab shows the progression of the states for the record.

The numerical value of the current state of the record is highlighted in the stepper component for reference as shown in the following example.




A typical record moves through the following progression of the states:

- **Draft**
- **In review**
- **Returned**
- **Pending approval**
- **Approved**
- **Archived**

If a record requires further updates and it is rejected by the approver of the record, it is set to the **Returned** state by the application software. When the record owner updates the details of the record, it follows the approval workflow again.

# Compliance Case Management

Report, investigate, analyze, and resolve a compliance case or raise compliance request by using the ServiceNow® GRC: Compliance Case Management application.

The Compliance Case Management application helps you to report, investigate, and resolve compliance cases , such as complaints and breaches. The Compliance Case Management

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

application provides a highly configurable workflow that is based on a compliance case or request.

| | | |
|---|---|---|
| Explore<br>  <br>Learn about how compliance case managers, compliance case analysts, and compliance case administrators use the Compliance Case Management application. | Configure<br>  <br>Configure your Compliance Case Management application. | Use<br>  <br>Create a compliance case, request, case tasks, and so on. |
| Reference<br>  <br>Get details about components like tables and roles. | | |

## Exploring Compliance Case Management

Learn how you can use the GRC: Compliance Case Management application to report, investigate, analyze, and resolve a compliance case, or raise a compliance request for your organization.

### Benefits of Compliance Case Management

The Compliance Case Management application offers the following benefits for your organization:

- Reporting, investigating, and resolving compliance cases or events, such as requests, complaints, and breaches.
- Raise a compliance request, such as policy modifications, clarifications, and inquiries.
- Recording the regulations that were violated by the event impact, with the event lodgment date.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

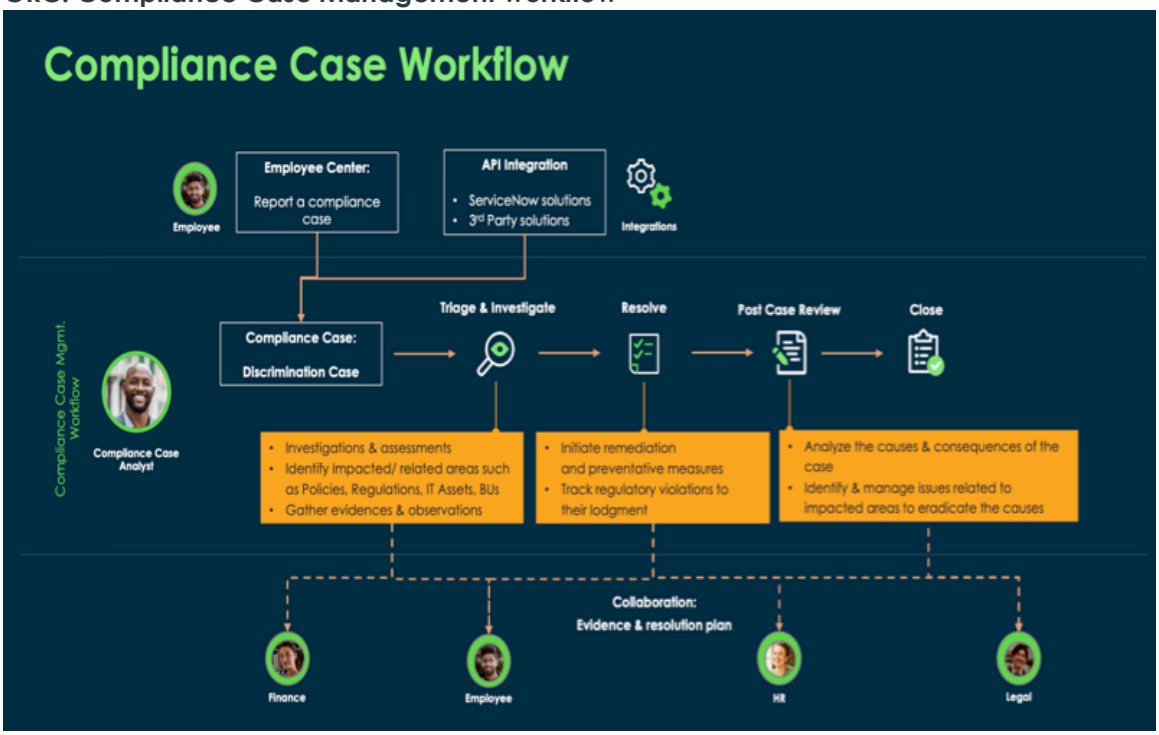
- Collaborate effortlessly with multiple teams to investigate and manage compliance cases and requests.
- Providing a highly configurable workflow that is based on a compliance case or request.

## Compliance case workflow

The workflow in the Compliance Case Management application is a process that enables you to report and manage cases that need the compliance team's attention.

The following diagram shows the workflow of the GRC: Compliance Case Management application.

**GRC: Compliance Case Management workflow**




The different stages of the compliance workflow are described as follows:

- Report a compliance case
- Triage the compliance case
- Investigate and evaluate the compliance case
- Resolve the compliance case
- Post case review and closure

## Report a compliance case

A business user or a compliance team reports a compliance violation. A business user can report a case in the Employee Center application. A compliance case team can report cases in the Compliance Workspace application. For more information, see Reporting a compliance case in GRC: Compliance Case Management.

## Triage the compliance case

After a compliance case is reported, the compliance team triages the case from a validity standpoint. The team then assigns a case analyst to work on the case.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Investigate and evaluate the compliance case

The compliance case analyst collaborates with multiple teams to investigate, gather evidence, and capture the details and responses about the case. Then, the case analyst creates the case tasks to initiate an investigation and assessment of a reported case and assigns them to a case task owner.

The case task owner adds the requested details and submits them to the case analyst for review. Based on the investigation and assessment responses, the case analyst performs the following tasks:

- Add the areas that are impacted by a compliance case. For example, the impacted areas or objects that could be impacted are the entities, controls, locations, or users that are affected by the compliance case. For more information, see Add an impacted area to a compliance case.
- Add the areas that are related to the compliance case. For example, the related areas include the policies, citations, control objectives, or risk events. For more information, see Add a related area to a compliance case.
- Add the compliance regulations that might be impacted to the compliance case. For more information, see Add compliance regulations to a compliance case.
- Add the causes and consequences of this compliance case such as the root cause for the reported compliance case or event and its consequences on the organization. For more information, see Add a cause and consequence to a compliance case.

## Resolve the compliance case

After all the analysis for the reported case is completed, the case analyst initiates the remediation actions and preventive measures to resolve the case. The case analyst also tracks the reportable regulatory violations to ensure their lodgment to the regulators.

## Post case review and closure

The case analyst analyzes the causes and consequences of the case. Then, the case analyst conducts a root-cause analysis to remove the cause of the case. The case analyst can review the case to identify and manage the issues that are related to the impacted areas. For more information, see Add or create an issue for a compliance case. Finally, the compliance analyst works closely with the various teams to review and close the compliance case.

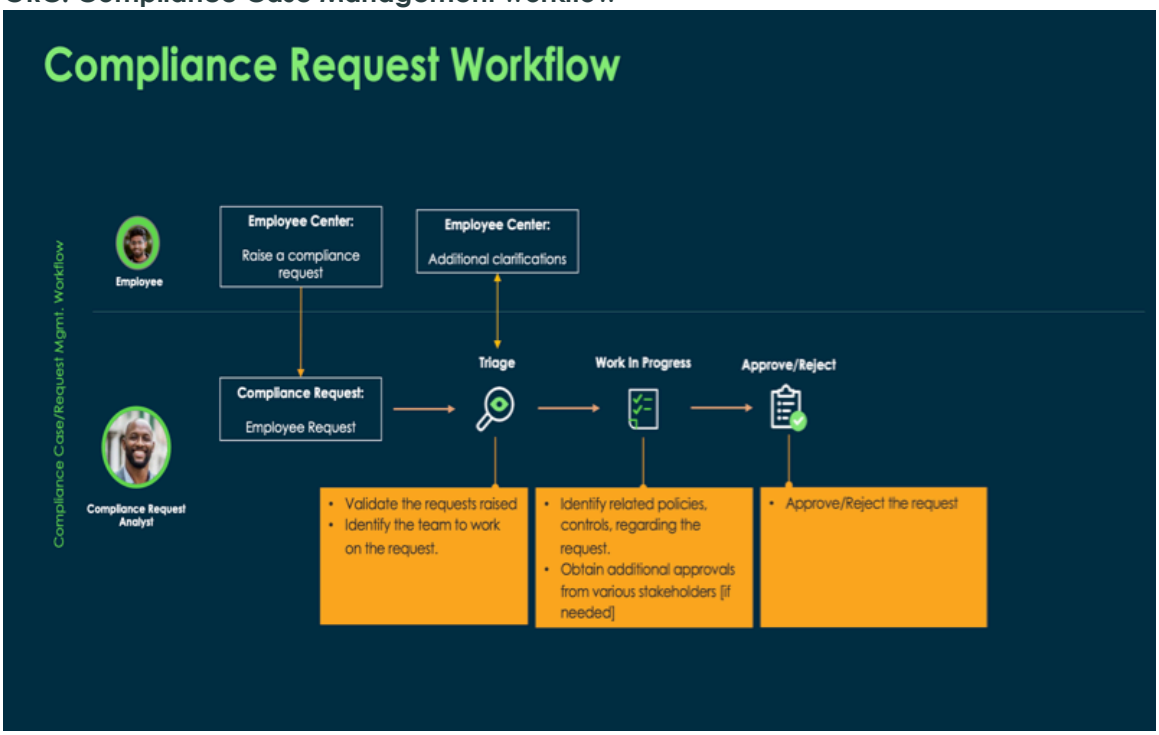
## Compliance request workflow

Use the request workflow in the Compliance Case Management application to raise and manage compliance requests within an organization. By using this workflow, your compliance requests are addressed effectively and efficiently by your compliance team.

The following diagram shows the workflow of a compliance request in the GRC: Compliance Case Management application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

GRC: Compliance Case Management workflow




The different stages of a compliance request are described as follows:

- Raise a compliance request
- Triage the compliance request
- Working on a compliance request
- Awaiting request approval
- Cancel a compliance request
- Close a compliance request

## Raise a compliance request

A business user or compliance team raises a compliance request. A business user can raise a request in the Employee Center application. A compliance case team can raise requests in the Compliance Workspace application. For more information, see Raising a compliance request in GRC: Compliance Case Management.

## Triage the compliance request

After a compliance request is raised, the compliance team assigns a request analyst to work on the case. The request analyst then triages the case from a validity standpoint. By conducting this evaluation, the request analyst ensures that only the valid and relevant requests proceed further in the compliance process. After the request analyst verifies the request as valid, the request moves to the In progress state.

## Working on a compliance request

In the In progress stage, the request analyst determines all the requirements for the raised request. The request analyst verifies the eligibility of the request and identifies any supporting documents, such as the policies, controls, citations, and control objectives that are related to the request. The case analyst can approve or reject the compliance request. If necessary, the analyst can seek approvals from the various stakeholders.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Awaiting request approval

After the request has been reviewed, it reaches this stage where a decision is made regarding its approval or rejection. This stage involves evaluating the raised request. If the request meets the necessary criteria, it's approved. Otherwise, it may be rejected with the justifications provided to the requester. Requests can be sent for approval to multiple users and can be approved or rejected by any one of them. The **Any Approvers** option enables the request to be closed as soon as it receives an approval or rejection from any of the assigned approvers. For more information, see Create an approval workflow.

## Cancel a compliance request

In this stage, a request may need to be canceled if it isn't a compliance request. A request can be canceled with the justifications provided to the requester. A request can be canceled at any stage, including Triage, In Progress, and Awaiting Approval states.

## Close a compliance request

After a compliance request is fully processed and approved or rejected, it enters the Closed stage. This stage indicates that all the necessary actions that are related to the request have been taken. The request is considered resolved, and no further actions are required.

## Compliance Case Management landing page

See an overview of all your compliance case-related information on your GRC: Compliance Case Management landing page. You can also create the cases, requests, and issues from this GRC: Compliance Case Management landing page.

## Overview

You can launch the compliance case management landing page by using the launcher (  ) icon.

The GRC: Compliance Case Management landing page consists of the following sections:

- Cases
- Requests
- My tasks

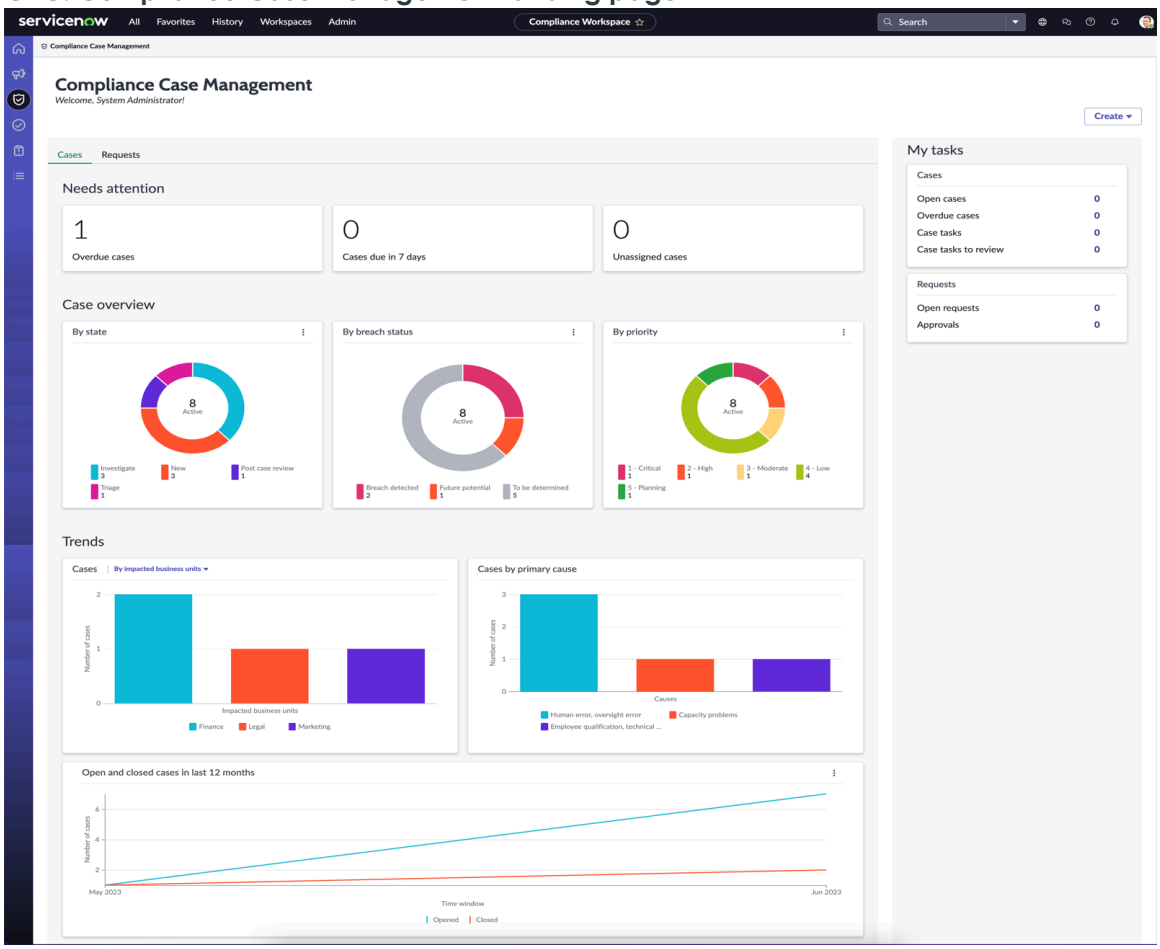
## Cases section

The Cases section includes the cards that offer information on compliance cases. You can see the cases that require attention, an overview, trends, and monitoring information.

The following example shows the cards that are available for the cases on the GRC: Compliance Case Management landing page.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## GRC: Compliance Case Management landing page




The following table describes the cards that are available for the cases on the GRC: Compliance Case Management landing page.

### Cases section

| Card | Description |
|---|---|
| Needs attention | Overview of the events or cases that need immediate attention:<br>Overdue cases<br>Cases where the closure date has been passed.<br>Cases due in 7 days<br>Cases where the closure date is in the next seven days.<br>Unassigned cases<br>Cases not assigned to a case analyst yet. |
| Case overview | Graphical representation of all the active cases by their state, breach status, and priority:<br>By state |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Cases section (continued)**

| Card | Description |
|---|---|
| | Shows the number of active cases by the workflow states that they're in. For example, as a compliance case manager, you can view the number of active cases that are under the investigation state.<br>By breach status<br>Shows the number of active cases only when a breach is detected, a chance of a breach is in the future, or the breach status is determined yet.<br>By priority<br>Shows the number of active cases by the priority that is defined at the case level. |
| Trends | Trends about your cases:<br>• Reported cases by the affected business units and geographical locations.<br>• Number of reported cases for each primary cause.<br>• Number of open and closed cases in the last 365 days. |
| Tracking | Items to track:<br>• Number of open issues for a compliance case<br>• Number of overdue issues<br>• Number of issues due in the next seven days |

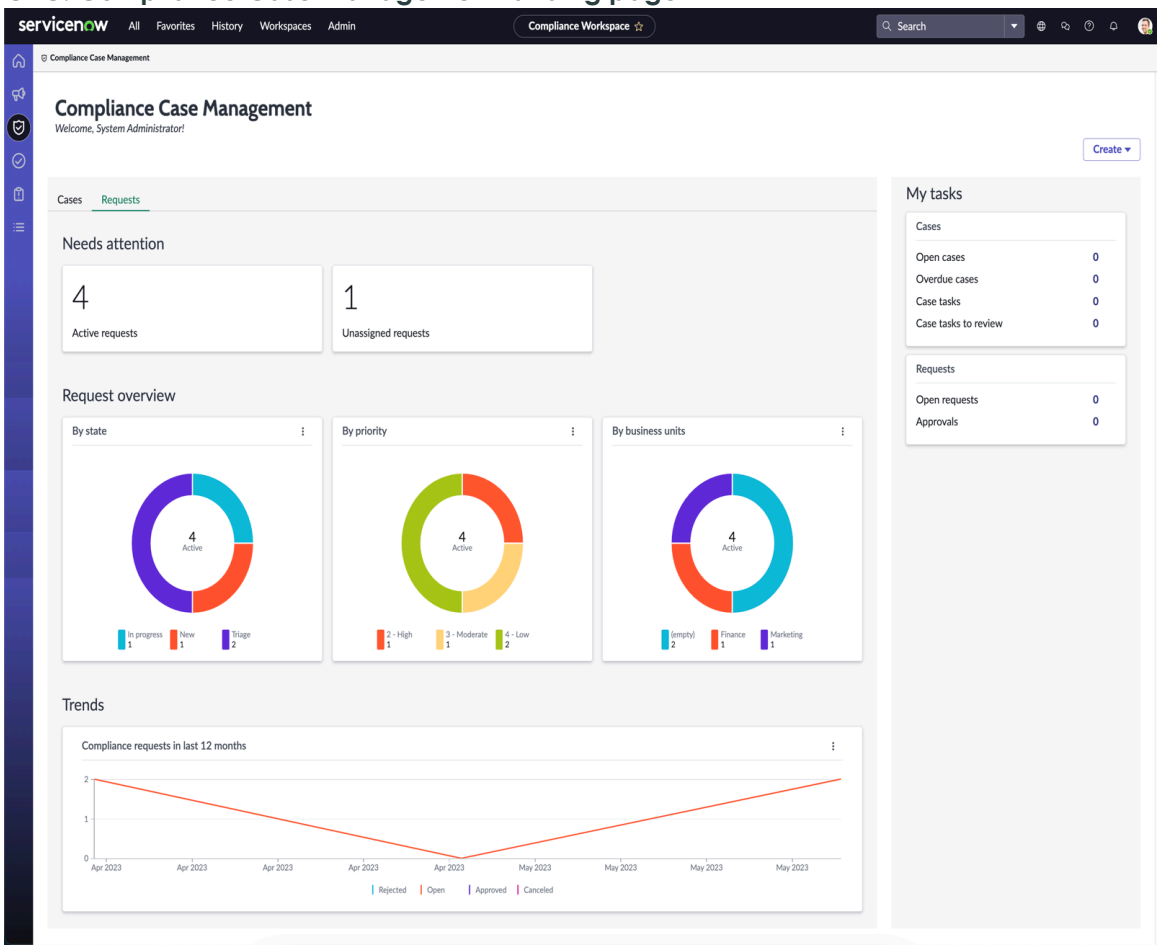
## Requests section

The Requests section includes the cards that offer information on compliance requests. You can see the requests that require attention, an overview, and trends.

The following example shows the cards that are available for the requests on the GRC: Compliance Case Management landing page.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## GRC: Compliance Case Management landing page




The following table describes the cards that are available for the requests on the GRC: Compliance Case Management landing page.

| Card | Description |
|---|---|
| Needs attention | Overview of the requests that need immediate attention:<br>Active requests<br>All open requests.<br>Unassigned request<br>Requests that aren't assigned yet. |
| Request overview | Graphical representation of all the active requests by their state, priority, and business units:<br>By state<br>Shows the number of active requests by the workflow states that they're in. For example, as a compliance case manager, you can view the number of active cases that are under the in progress state. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Card | Description |
| --- | --- |
| | By priority<br>Shows the number of active requests by the priority that is defined at the request level.<br>By business units<br>Shows the number of active requests categorized by the business units. |
| Trends | Number of compliance requests that are open, approved, rejected, and canceled in the last 12 months. |

## My tasks section

My tasks section consists of the individual sections for cases and requests.

In the Cases section, you can access all the cases and tasks that are assigned to you:

Open cases
: All the cases that are assigned to you.

Overdue cases
: Any overdue cases that are assigned to you.

Case tasks
: All the case tasks that are assigned to you to work on.

Case tasks to review
: Pending case tasks that you need to review. For example, let's say that as a case analyst, you've created a case task and assigned it to a case task owner to work on it. The case task owner completed the case task and submitted it to you for review. Now, you need to review and complete these case tasks.

In the Requests section, you can access all the requests that are assigned to you:

Open requests
: All the requests that are assigned to you.

Approvals
: All the requests that are awaiting your approval.

## Using the compliance case overview related list

The compliance case overview related list shows the details about a case. For example, you can see the description, state, schedule and milestones, case tasks, and issues that are related to a case in the GRC: Compliance Case Management application.

The Compliance Case Management overview related list includes the following sections:

- Description
- State
- Case schedules and milestones
- Case tasks overview

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Tracking
- Attachments

### Description section

The Description section includes the detailed information that you can fill in when you're creating a compliance case. For example, you can add the purpose, action being taken, time line, applicable rules and regulations, and any relevant evidence or documents. By using this section, you can understand the context of the case and take the necessary steps to resolve it.

### State section

The State section includes the workflow states of a compliance case. For example in this section, you see various stages of the compliance case, such as New, Triage, Investigate, Resolve, Post case review, and Close. These states determine the status of the case. A compliance case administrator can configure these states in the GRC: Compliance Case Management application. For more information, see Create a state model to define the workflow states and transitions.

### Case schedules and milestones section

The Case schedules and milestones section includes the details on all the milestones or events during the case life cycle in a time-line range. In this section, you can see an outline of the key events, such as the date when the case was reported, occurred, discovered, or closed. You can also filter the events to view the following options on the time-line range after you select the **Show events** option:

Case creation date
: Date when the case was created.

Date of discovery
: Date when the case was discovered.

Date of occurrence
: Date when the case occurred.

Milestone
: Dates related to the investigation remediation milestones.

Breach
: Dates related to the breach analysis.

Today
: Current date on the time line.

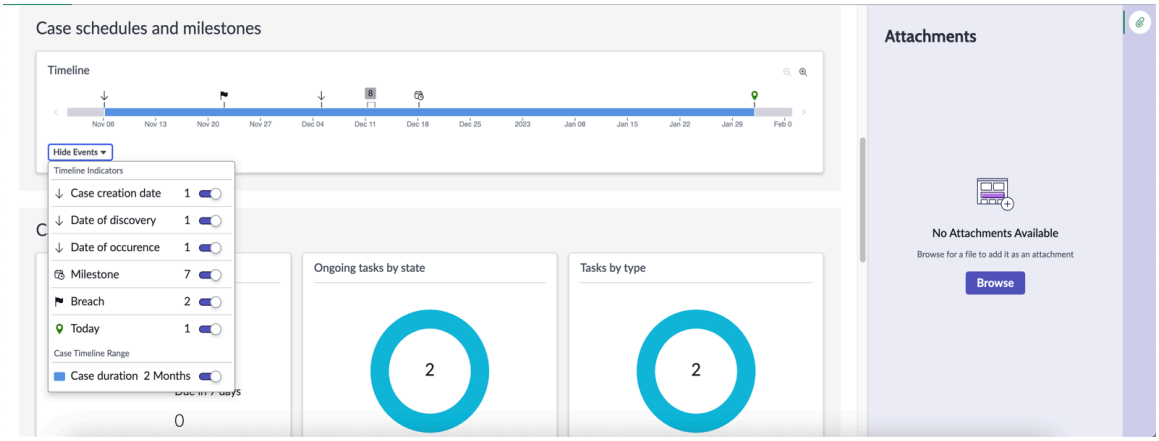
Case closure
: Date when the case was closed or met the case closure service level agreement (SLA).

Case duration
: Date when the case was created to the last milestone date.

The following example shows the options available after you select the **Show events** option.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Case schedules milestones




**Note:** The options that are displayed after you select the **Show events** option are limited to the events and milestones that are available for the case.

## Case tasks overview section

The case task overview section includes the following subsections:

Tasks

Total number of case tasks, any overdue case tasks, and case tasks that are due in seven days.

Ongoing tasks by state

Number of active case tasks by the states.

Tasks by type

Number of active case tasks by the case type.

## Tracking section

The Tracking section displays the following information:

- Number of open issues for a compliance case
- Number of overdue issues
- Number of issues due in the next seven days

## Attachments section

The Attachment section enables you to upload a file as an attachment to a case. In this section you can find all the attachments that have been added.

## 360° Relationship Visualization of a compliance case

Use the 360° compliance case view to explore the relationship between your compliance case and all its associated objects in a distinctive visualization. To use this feature, you must integrate Compliance Case Management with the 360° Relationship Visualization application.

## 360° view of a compliance case

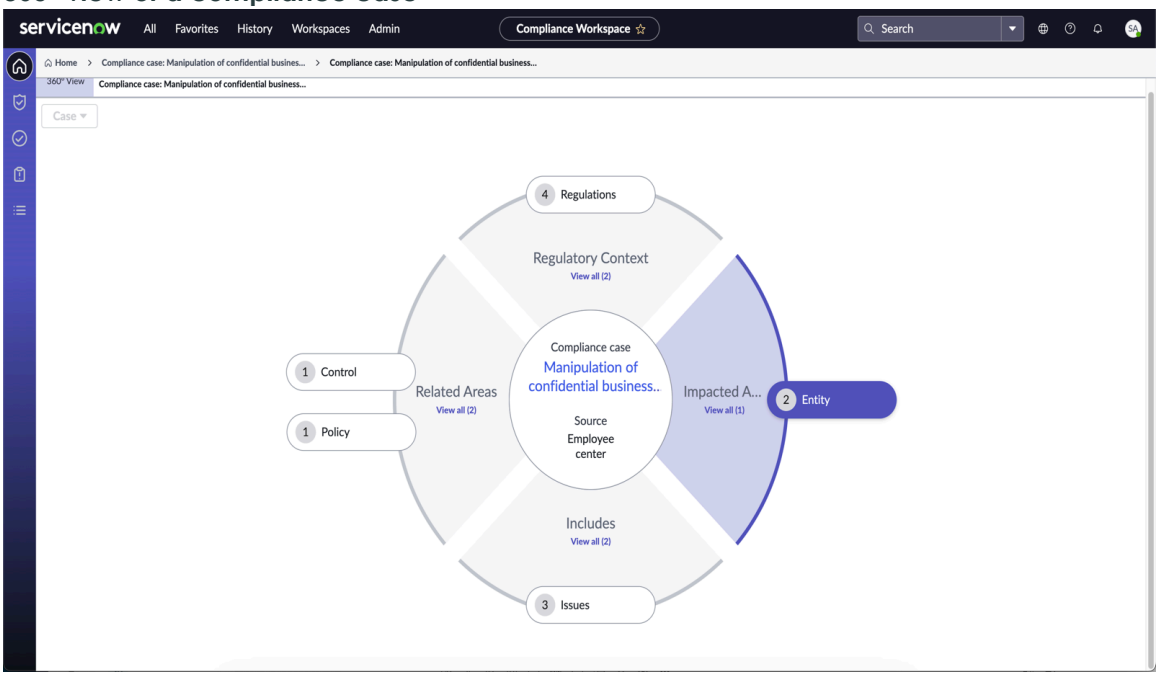
When you launch the 360° view from a compliance case record, you can visualize the relationships between the selected record and all its associated objects. This visualization provides valuable insights into how these objects interact and relate to each other within

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the compliance case. You can take actions on the displayed records. For example, you can dive deeper to explore more information or create records.

The following example shows the 360° view of a compliance case:

**360° view of a compliance case**




To explore the 360° view and to learn how to launch the view, see Exploring the 360° view.

To learn more about the users who could use 360° Relationship Visualization, their roles, and responsibilities, see 360° Relationship Visualization.

## 360° view of compliance objects integrated with compliance case

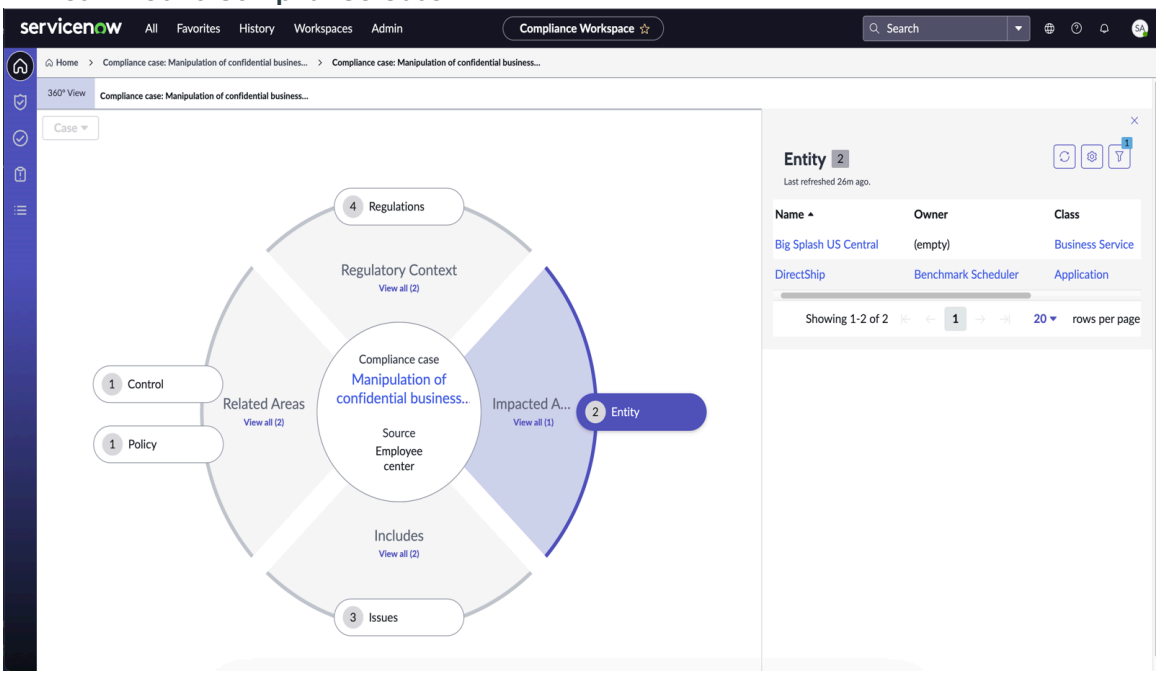
The 360° view of a compliance case record offers a comprehensive and detailed perspective on the various objects that are associated with the case. The associated objects are entities, citations, regulations, case tasks, issues, controls, and policies. For example, when you select the Entity option, it enables you to explore the list of entities that are related to the compliance case. You can also view the source from where the compliance case has been raised.

The 360° view enables you to access information about the source from which the compliance case has been raised.

The following example shows the entities linked to a compliance case:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Entities linked to compliance case




# Configuring Compliance Case Management

You can configure the Compliance Case Management application to report, investigate, analyze, and resolve a compliance case or requests.

Follow the order of the tasks here to configure the GRC: Compliance Case Management application. These tasks help you to manage the compliance cases and requests effectively.

## Download Compliance Case Management

Before you run the Compliance Case Management application in your instance, you must download it from the ServiceNow Store.

### Before you begin

Role required: admin

### About this task

The ServiceNow Store application enables you to download the core products and applications. A product contains one or more applications that are licensed as a group. For example, the GRC application is a product.

### Procedure

1. In the ServiceNow Store application, you must ensure that you have entitlements, or licenses, to the application and its dependent applications.

   **Note:** This process applies only to the applications that are downloaded to the production instances. If you're downloading the applications to your non-production or development instances, it isn't necessary to get entitlements. Proceed to Activate a ServiceNow Store application.

2. Activate the application and run it on your instance.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Install Compliance Case Management

You can install the GRC: Compliance Case Management application (sn_comp_case) if you have the admin role.The application includes the demo data and related ServiceNow® Store applications and plugins if they aren't already installed.

### Before you begin

Role required: admin

Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.

### About this task

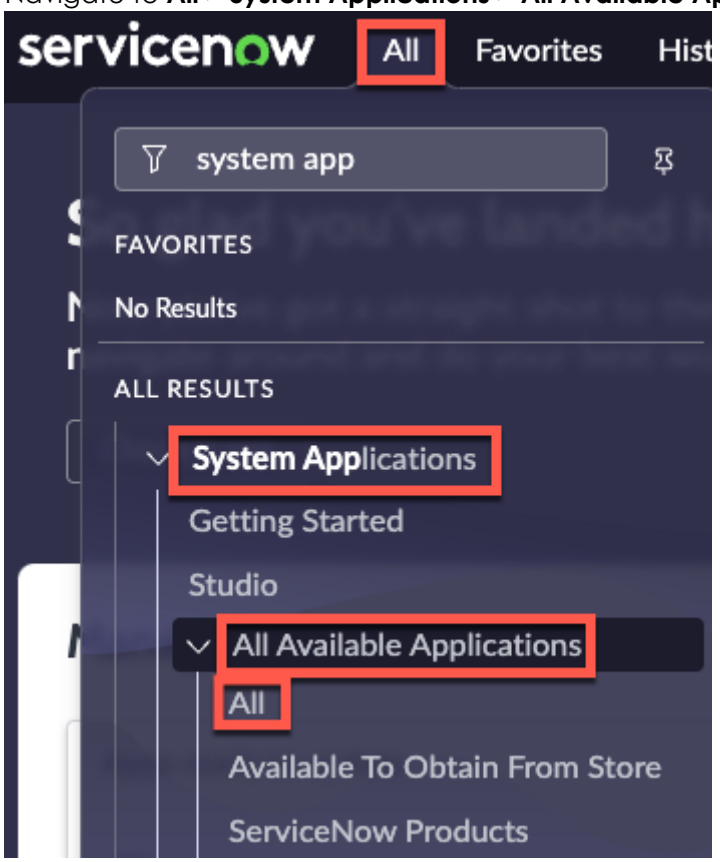
The following items are installed with Compliance Case Management:

- Plugins
- Store applications
- Roles
- Scheduled jobs
- Tables

For more information, see Tables installed with Compliance Case Management and Roles installed with Compliance Case Management.

### Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Find the Compliance Case Management application (sn_comp_case) by using the filter criteria and search bar.

   You can search for the application by its name or ID. If you can't find the application, you might have to request it from the ServiceNow Store.

   In the list next to the **Install** button, the versions that are available are displayed.

3. Select a version from the list and select **Install**.

   In the Install dialog box that is displayed, any dependencies that are installed along with your application are listed.

4. If you are prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.
5. Optional: If demo data is available and you want to install it, select the **Load demo data** check box.
   Demo data comprises the sample records that describe application features for the common use cases. Load the demo data when you first install the application on a development or test instance.

   **Important:** If you don't load the demo data during installation, it's unavailable to load later.

6. Select **Install**.

## Create a case type

Create a case type in the GRC: Compliance Case Management application to categorize the compliance cases by the type of occurrence. For example, you can create a case type, such as a financial case, code of conduct, or HR case.

### Before you begin

Role required: sn_compliance_case_admin

### About this task

You can set up a case type to categorize the compliance cases by the type of occurrence. After you define the case type, the compliance analyst and compliance manager can select the case type on the case form. A case type is mapped with a state model that specifies the workflow states and transition conditions for the compliance case. To define the workflow states and transitions, see Create a state model to define the workflow states and transitions.

### Procedure

1. Navigate to **All** > **Compliance Case Management** > **Case types**.
2. Select **New**.
3. On the form, fill in the fields.

   For a description of the field values on the case type form, see Case Type form.

4. Open the form context menu and select **Save**.
   The Case subtypes related list appears.
5. On the Case subtypes related list, select **New** to define a case subtype.
6. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Case Subtype form**

| Field | Description |
|---|---|
| Label | Label to be displayed for the case subtype. |
| Name | Name of the case subtype. For example, Conflict of interest. |
| Parent | Parent case type. This field is automatically set to the parent case type. |
| Active | Option to select the case subtype as active or inactive. |
| Description | Description of the purpose of the case subtype. This description is for the administrator to understand the case subtype. |

7. Select **Submit**.
8. Optional: To create a view rule instead of using the default one, see Create a view rule.
9. Optional: To create an assignment rule instead of using the default one, see Create an assignment rule.

### Case Type form

Use the Case Type form in the Compliance Case Management application to categorize the compliance cases by their type.

See the following table for a description of the field values.

**Case Type form**

| Field | Description |
|---|---|
| Label | Label to be displayed for the case type. |
| Name | Name of the case type. For example, Code of conduct. |
| Case category | Category of the case type. This field is automatically set to **Compliance case [sn_comp_case_compliance_case]**. |
| Active | Option to select the case type as active or inactive. |
| Description | Description about this case type. This description is for the administrator to understand the case subtype. |
| State Model | |
| State Model | Workflow states for the case type. For more information, see Create a state model to define the workflow states and transitions. |
| Assessment Configuration | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Case Type form (continued)**

| Field | Description |
|---|---|
| Assessment templates | Assessment template for the case type. For more information, see Create an assessment template. |
| Template Configuration | |
| Document templates | Template to generate Portable Document Format (PDF) reports for compliance cases associated with this case type. |

### Create a view rule

Define the view rules for the workspace and default view in the GRC: Compliance Case Management application. By defining the rules, you can control how the compliance case or request form appears.

#### Before you begin

Role required: sn_compliance_case_admin

#### Procedure

1. Navigate to **All** > **Compliance Case Management** > **Case types**.
2. Open a case type from the list.
3. On the case type form, select **View Rules**.
4. Select **New**.
5. On the form, fill in the fields.
   For a description of the field values on the View Rule form, see View Rule form.
6. Select **Submit**.

### View Rule form

Use the View Rule form to define the workspace and default view rules in the GRC: Compliance Case Management application.

See the following table for a description of the field values.

**View Rule form**

| Field | Description |
|---|---|
| Name | Name to identify the rule. |
| Table | Table that this view rule applies to. This field is automatically set to **Compliance case [sn_comp_case_compliance_case]**. |
| View | View option that you're creating a rule for:<br>• **Default view**: Define the form view on the Classic environment.<br>• **Workspace**: Define the form view on Workspace. |
| Experience Restricted | Option to enable this view rule to one or multiple workspaces. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**View Rule form (continued)**

| Field | Description |
|---|---|
| Application | Name of the application that this view rule applies to. This field is automatically set to **GRC: Compliance Case Management**. |
| Execution Order | Order in which this view rule executes. |
| Active | Option to enable the view rule. |
| Conditions | |
| Roles | Roles that this view rule applies to. |
| Conditions | Condition builder to set conditions for the view rule. |
| Form Settings | |
| Hide details & UI actions | Option to hide the **Details** tab in the related list. |
| Hide Journal Input Fields | Option to disable the journal fields on the Workspace forms. |
| Hide section navigation | Option to disable the jump-to section navigation on the Workspace forms. |
| Disable section collapsing | Option to disable the default form section collapse. |
| Form Tabs | |
| Default Tab Order | Option to select the default tab order on the Workspace form. |
| Tab Order | Option to define the tab order on the Workspace form. This field appears only when you deselect the **Default Tab Order** option. |
| Default Tab Focus | Item that should be in focus when you open a record in the table that is specified in this rule. |

### Create an assignment rule

Create an assignment rule and apply it to a compliance case type or request type by using the Compliance Case Management application. By using an assignment rule, you can determine the appropriate person or group to handle a compliance case.

#### Before you begin

Role required: sn_compliance_case_admin

#### About this task

You can create an assignment rule to assign the case or request to a user or group by the pre-defined conditions.

#### Procedure

1. To define assignment rule for a case type, navigate to **All** > **Compliance Case Management** > **Case types**.
2. To define assignment rule for a request type, navigate to **All** > **Compliance Case Management** > **Request types**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Open a case or request type from the list.
4. On the case type or request type form, select **Assignment Rules**.
5. Select **New**.
6. On the form, fill in the fields.
   For a description of the field values on the Assignment Rule form, see Assignment Rule form.
7. Select **Submit**.

### Assignment Rule form

Use the Assignment Rule form to define the case assignment rules in the Compliance Case Management application.

See the following table for a description of the field values.

**Assignment Rule form**

| Field | Description |
|---|---|
| Name | Name of the assignment rule. |
| Application | Name of the application that this assignment rule applies to. This field is automatically set to **GRC: Compliance Case Management**. |
| Active | Option to enable the assignment rule. |
| Applies to | |
| Table | Table that this assignment rule applies to. This field is automatically set to **Compliance case [sn_comp_case_compliance_case]**. |
| Conditions | Condition builder to set conditions for the assignment rule. |
| Assign to | |
| User | User that the case or request is assigned to. |
| Group | Group that the case or request is assigned to. |
| Script | |
| Script | Script to define the advanced assignment rule. |

## Create a request type

Create a request type in the GRC: Compliance Case Management application to categorize and manage the compliance requests. After you create a request type, the compliance analysts and managers can select the required request type on the request form.

### Before you begin

Role required: sn_compliance_case_admin

### Procedure

1. Navigate to **All** > **Compliance Case Management** > **Request types**.
2. Select **New**.
3. On the form, fill in the fields.

   For a description of the field values on the request type form, see Request type form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Open the form context menu and select **Save**.
   The Subtypes related list appears.
5. On the Subtypes related list, select **New** to define a request subtype.
6. On the form, fill in the fields.

**Subtype form**

| Field | Description |
|---|---|
| Label | Label to be displayed for the subtype. |
| Name | Name of the subtype. For example, Policy update. |
| Parent | Parent request type. This field is automatically set to the parent request type. |
| Active | Option to select the subtype as active or inactive. |
| Case category | Category of the subtype. This field is automatically set to **Compliance case [sn_comp_case_compliance_request]**. |
| Description | Description of the purpose of the subtype. This description is for the administrator to understand the request subtype. |

7. Select **Submit**.
8. Optional: To create a view rule instead of using the default rule, see Create a view rule.
9. Optional: To create an assignment rule instead of using the default rule, see Create an assignment rule.

### Request type form

Use the Request Type form in the Compliance Case Management application to categorize the compliance requests by their type.

The following table lists the descriptions of the field values.

**Request Type form**

| Field | Description |
|---|---|
| Label | Label to be displayed for the request type. |
| Name | Name of the request type. For example, Policy update/enquiry. |
| Category | Category of the request type. This field is automatically set to **Compliance case [sn_comp_case_compliance_request]**. |
| Active | Option to select the request type as active or inactive. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Request Type form (continued)**

| Field | Description |
|---|---|
| Description | Description about this request type. This description is for the administrator to understand the request type. |
| State Model | |
| State Model | Workflow states for the request type. For more information, see Create a state model to define the workflow states and transitions. |
| Template Configuration | |
| Document templates | Template to generate Portable Document Format (PDF) reports for compliance requests associated with this request type. |

## Create a state model to define the workflow states and transitions

Create a state model to define the workflow states and transition conditions for compliance case types and request types.

### Before you begin

Role required: sn_compliance_case_admin

### About this task

A state model is a list of states that describe the workflow of a record. With a state model, you can define the state transitions for a specific case or request type. The case type or request type follows the workflow states and transition conditions that are defined in the state model.

### Procedure

1. Navigate to **All** > **Compliance Case Management** > **State Models**.
2. Select **New**.
3. On the form, fill in the fields.

   For a description of the field values on the GRC State Model form, see GRC State Model form.

4. Select **Submit**.

#### GRC State Model form

Use the GRC State Model form to define the workflow states and transition conditions in the Compliance Case Management application.

See the following table for a description of the field values.

**GRC State Model form**

| Field | Description |
|---|---|
| Name | Name of the state model. For example, Breach case. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**GRC State Model form (continued)**

| Field | Description |
|---|---|
| Application | Name of the application that this state model applies to. This field is automatically set to **GRC: Compliance Case Management**. |
| Active | Option to select the state model as active or inactive. |
| Table | Table that this state model applies to. This field is automatically set to **Compliance case [sn_comp_case_compliance_case]**. |
| State Model | Field to hold the state model value in a table that this state model applies to. |
| State | Field to hold the state value in a table that this state model applies to. This field is automatically set to **State**. |

## Create a workflow state for a compliance case or request

Create a workflow state for a compliance case or request to define the life cycle of the case or request using the Compliance Case Management application.

### Before you begin

Role required: sn_compliance_case_admin

### Procedure

1. Navigate to **All** > **Compliance Case Management** > **State Models**.
2. Open the state model that you want to add the workflow to.
3. On the GRC workflow states context menu, select **New**.
4. On the form, fill in the fields.

   For a description of the field values on the Workflow state form, see Workflow State form.
5. Select **Submit**.

#### Workflow State form

Use the Workflow State form to define the workflow states in the GRC: Compliance Case Management application.

See the following table for a description of the field values.

**Workflow State form**

| Field | Description |
|---|---|
| State | Name of the workflow state for compliance case:<br>• **New**<br>• **Triage**<br>• **Investigate** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Workflow State form (continued)**

| Field | Description |
|---|---|
| | • **Resolve**<br>• **Post case review**<br>• **Close**<br>• **Canceled**<br><br>Name of the workflow state for compliance request:<br>• **New**<br>• **Triage**<br>• **In progress**<br>• **Canceled**<br>• **Awaiting approval**<br>• **Approved**<br>• **Rejected**<br>• **Closed** |
| Application | Name of the application that this view rule applies to. This field is automatically set to **GRC: Compliance Case Management**. |
| Model | State model that uses this workflow state. This field is automatically set to the state model name. |
| Display type | Display type option of the workflow state:<br>• **As node**: Option to select as a parent state.<br>• **As sub-level**: Option to select as a sub-state of the parent state. |
| Is optional | Option to select the state as optional. This field appears only when **As node** is selected from **Display type**. |
| Stepper label | Label to be displayed on the stepper component for the state. This field appears only when **As sub-level** is selected from **Display type**. |
| Parent model state | Parent state for the sub-level state. This field appears only when **As sub-level** is selected from **Display type**. |

## Define the model state transitions for a compliance case or request

Define the transition conditions to control how a compliance case traverses through the different workflow states by using the GRC: Compliance Case Management application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_compliance_case_admin

### About this task
The state transitions are a list of conditions for entering or exiting each state that is defined for a table. In the State Transitions table, use the condition builder to build a list of required conditions for entering or exiting each state.

### Procedure
1. Navigate to **All** > **Compliance Case Management** > **State Models**.
2. Open the state model that you want to define the model state transition for.
3. To define the model state transition, select the required workflow state.
4. On the Model State Transitions context menu, select **New**.
5. Select the state that you want to move to from the selected state.
6. Optional: To enable the automatic transition of the workflow state, select the **Automatic transition** option.
7. Open the form context menu and select **Save**.
   The GRC model state transition conditions related list appears.
8. On the GRC model state transition conditions context menu, select **New**.
9. On the form, fill in the fields.

   For a description of the field values on the GRC model state transition form, see GRC Model State Transition Condition form.
10. Select **Submit**.

#### GRC Model State Transition Condition form
Use the GRC Model State Transition Condition form to define the transition conditions to control how a compliance case or request traverses through the different workflow states by using the GRC: Compliance Case Management application.

See the following table for a description of the field values.

#### GRC Model State Transition Condition

| Field | Description |
|---|---|
| Name | Name of the condition. |
| State transition | Transition of states. This field is automatically set to the model state transition value. |
| Application | Name of the application that this condition applies to. This field is automatically set to **GRC: Compliance Case Management**. |
| Active | Option to enable the model state transition condition. |
| Description | Description of this state transition. For example, in the **Description** field for the New state, you could enter `New state can move only to Analyze state`. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**GRC Model State Transition Condition (continued)**

| Field | Description |
|---|---|
| Error message | Error message to be displayed when the conditions aren't met. |
| Requires | Transition conditions:<br>• **Task has been through Approval**: Condition passes if the related task has an approval that is either accepted or rejected.<br>• **Task is Approved**: Condition passes when the task is approved.<br>• **Task is Rejected**: Condition passes when the task is rejected.<br>• **Transition Condition**: Conditions for this state transition.<br>• **Transition Script**: Advanced conditions for this state transition. |
| Condition | Conditions to be defined for this state transition. This field appears only when **Transition Condition** is selected from **Requires**. |
| Script | Script to be defined for this state transition. This field appears only when **Transition Script** is selected from **Requires**. |

## Create an assessment template

Create an assessment template to request responses from the assessor or reviewer. You can create this template by using the assessment metric type form in the GRC: Compliance Case Management application.

### Before you begin

Role required: sn_compliance_case_admin

### About this task

You can create a questionnaire template instead of using the default template to assess your compliance cases. After you set up the assessment template, it's available in the case task section for that case type.

### Procedure

1. Navigate to **All** > **Compliance Case Management** > **Assessment Templates**.
2. Select **New**.
3. On the form, fill in the fields.
   For a description of the field values on the Assessment Metric Type form, see Assessment Metric Type form.
4. Select **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Assessment Metric Type form

Use the Assessment Metric Type form to create an assessment questionnaire template by using the GRC: Compliance Case Management application.

See the following table for a description of the field values.

**Assessment Metric Type form**

| Field | Description |
|---|---|
| Name | Name of the assessment template. |
| Assessment duration | Length of time allowed for completing the assessment from the time that the assessment is generated. |
| Table | Table that contains the records. This field is automatically set to **GRC core case [sn_grc_case_mgmt_core_case]**. |
| State | State of the assessment. This field is automatically set to **Draft**. |
| Roles | Roles who can view the results and access records that are associated with this template. |
| Description | Purpose of the assessment template and the reason for its creation. |
| Introduction | Guidance text for business users who respond to the assessment. |

# Using Compliance Case Management

Report compliance cases and manage the lifecycle of a case by using the GRC: Compliance Case Management application.

## Reporting a compliance case in GRC: Compliance Case Management

You can report a compliance case or an event that needs the attention of the compliance team by using the GRC: Compliance Case Management application.

As a business user, you can report a case by using one the following options:

- Report a compliance case from the Employee Center
- Create a compliance case in the Compliance Workspace

### Report a compliance case from the Employee Center

Report any violation of the organization's policies or guidelines by using the Employee Center application. By reporting a case, you reduce and avert the adverse regulatory actions that could impact the company's financials, reputation, and growth.

#### Before you begin

Role required: sn_grc_emp_user.grc_employee or sn_comp_case.compliance_case_business_user

#### Procedure

1. Navigate to **All** > **Self-Service** > **Employee Center**.
2. On the Employee Center landing page, select the **Risk & Compliance** tab.
3. In the Browse Risk & Compliance section, select **Report a compliance case**.
4. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For a description of the field values on the Report a compliance case form, see Report a Compliance Case form.

5. Optional: On the Report a compliance case form, select **Add attachments** to attach supporting material or evidence.
6. Select **Submit**.

### Report a Compliance Case form

Use the Report a Compliance Case form in the Employee Center to report a compliance case.

See the following table for a description of the field values.

**Report a Compliance Case form**

| Field | Description |
|---|---|
| Title | Name of the case. For example, Verdict of a lawsuit leaked. |
| Description | Brief description of the case. |
| Case type | Type of the reported case. This field is automatically set to **Compliance case**. |
| Case subtype | Subtype of the reported case. For example, Data theft/Loss. |
| Date of occurrence | Date when the case occurred. For example, the case may have occurred on 18-02-2022. |
| Date of discovery | Date when the case was discovered. For example, the case may have occurred on 18-02-2022, but is discovered by you on 12-03-2022. |
| Case origin | |
| Impacted business unit | Business unit that is impacted by the reported case or event. |
| Location of occurrence | Location of the case occurrence. For example, the location is Japan. |
| Impacted department | Department that is affected by the case. For example, Customer support. |
| Sub-location of occurrence | Sub-location of the case occurrence. For example, the sub-location is Tokyo. |

### Create a compliance case in the Compliance Workspace

Report any violation of the organization's policies or guidelines by using the Compliance Case Management application. By reporting a case, you reduce and avert the adverse regulatory actions that could impact the company's financials, reputation, and growth.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst and sn_compliance_ws.corporate_compliance_manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

At times, your users can also report a case to the compliance teams through phone calls or emails. The compliance teams can then create these cases in the Compliance Workspace and attach the relevant details to the case.

### Procedure

1. Navigate to **All** > **Compliance Workspace**.
2. Select the Compliance case management icon (  ).
3. On the Compliance Case Management landing page, select **Create**.
4. From the options available in **Create**, select **Case**.
5. On the form, fill in the fields.
   For a description of the field values on the Create a Compliance Case form, see Compliance Case form.
6. Select **Save**.

### Compliance Case form

Use the Create Compliance Case form in the GRC: Compliance Case Management application to report a compliance case.

See the following table for a description of the field values.

#### Create Compliance Case form

| Field | Description |
|---|---|
| Number | Number of the case. This field is automatically set to a case number. |
| Title | Name of the case. For example, Verdict of a lawsuit leaked. |
| Type | Type of the case. This field is automatically set to **Compliance case**. |
| State | Workflow state of the case. This field is automatically set to **New**. |
| Requester | Person who reported the case. |
| Primary entity | Entity that is affected by the case. This field is automatically set to the entity that is identified in the Impacted areas related list. |
| Sub-type | Sub-type of the case. For example, Fraud and Embezzlement. |
| Priority | Priority of the case:<br>• **1 - Critical**<br>• **2- High**<br>• **3 - Moderate**<br>• **4 - Low**<br>• **5 - Planning** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create Compliance Case form (continued)**

| Field | Description |
|---|---|
| Requested on behalf of | Name of the person you created the case for. |
| Entity owner | User who is the owner of the entity. This field is automatically set based on the entity that is selected in the Impacted areas related list. |
| Description | Brief description of the case. |
| Assignment | |
| Assignment group | Group that is assigned to the case.<br>**Note:** The assignment group is preconfigured to the case type during the configuration setup. |
| Case analyst | Analyst who can analyze and work on the case. The case analyst is a part of the assignment group. |
| Watch list | User who must be informed about the case. |
| Accountable executive | Executive who is accountable for the case. |
| Primary origin | |
| Location | Location where the case occurred. For example, Japan. |
| Impacted business unit | Business unit that is affected by the reported cases or events. For example, Finance. |
| Source | Source from which the case is reported:<br>• **Manual**: When the case is created from the compliance workspace, the field displays the source as **Manual**.<br>• **Employee Center**: When the case is reported from the Employee Center, the field displays the source as **Employee Center**. |
| Additional source | Mode of how the case is reported when the case is created manually. This field is available only when **Manual** is selected from the **Source** field and the record is saved. The choices are as follows:<br>• **Email**: When you create the case from the information that you received in an email.<br>• **Phone**: When you create the case from the information that you received in a phone call. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create Compliance Case form (continued)**

| Field | Description |
|---|---|
| Sub-location | Sub-location of the case occurrence. For example, the sub location is Tokyo. |
| Impacted department | Department that is affected by the case. For example, Customer support. |
| Source record | Source record of the source object from where the case is created. For example, if the case is reported from risk events, then this field displays the name of the risk event from which the case is reported. |
| Schedule | |
| Date of occurrence | Date when the case occurred. For example, the case may have occurred on 18-02-2022. |
| Date of discovery | Date when the case was discovered. For example, the case may have occurred on 18-02-2022, but was discovered on 12-03-2022. |
| Case creation date | Date when the case was created. This field is automatically set to the current date and time. |
| Case closure SLA | Expected date of the case closure. |
| Investigation planned start | Planned start date to investigate the case. |
| Investigation planned end | Planned end date to investigate the case. |
| Investigation actual start | Actual start date of the case investigation. |
| Investigation actual end | Actual end date of the case investigation. |
| Remediation planned start | Planned start date to remediate the case. |
| Remediation planned end | Planned end date of the case remediation. |
| Remediation actual start | Actual start date of the case remediation. |
| Remediation actual end | Actual end date of the case remediation. |
| Breach analysis | |
| Breach status | Status to indicate if a breach has occurred or not:<br>• **To be determined**: When the breach isn't determined yet.<br>• **Breach detected**: When the breach is confirmed.<br>• **Future potential**: When the breach hasn't occurred but may occur in the future.<br>• **Not a breach**: When no breach is detected. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create Compliance Case form (continued)

| Field | Description |
|---|---|
| Reporting status | Status of the case being reported to the regulators. This field is automatically set based on the reporting status of the regulations that are associated with the case. If a case has many regulations and even if one regulation is identified as reportable, then the reporting status of the case is set to reportable. The default value of this field is **To be determined**. |
| Breach start | Date that the breach started. This field only appears when **Breach detected** or **Future potential** is selected from **Breach status**. |
| Breach end | Date that the breach ended. This field only appears when **Breach detected** or **Future potential** is selected from **Breach status**. |
| Breach severity | Intensity of the breach:<br>• **Critical**<br>• **High**<br>• **Medium**<br>• **Low** |
| Breach significance identified | Date when the user identifies that the breach is significant. This field only appears when **Breach detected** or **Future potential** is selected from **Breach status**. |
| Root cause analysis | |
| Primary cause | Primary cause of the case reported. This field is automatically set to the primary cause that is selected in the Cause and consequences related list. |
| Consequences | Consequences from the primary cause of the case reported. For example, damage to physical assets. |
| Overall observations | Observations made regarding the case. |
| Remediation taken | Option to indicate if the remediation measures have been taken to address the case:<br>• **Yes**<br>• **No** |
| Overall preventive measures | Preventive measures taken to remediate the case. |
| Activity | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create Compliance Case form (continued)**

| Field | Description |
|---|---|
| Work notes (Private) | Notes or information about the case. |
| Additional comments (Customer visible) | Additional information about the case that you want to share with the customers. |

## Raising a compliance request in GRC: Compliance Case Management

You can raise a compliance request to the compliance team by using the GRC: Compliance Case Management application. For example, you can submit a compliance request to seek advice or guidance on the organization's policies and guidelines.

You can raise a compliance request by using one the following options:

- Raise a compliance request from the Employee Center
- Create a compliance request in the Compliance Workspace

### Raise a compliance request from the Employee Center

Raise a compliance request regarding organization's policies, inquiries, and guidelines by using the Employee Center application. By seeking guidance, clarification, or approval, you contribute to maintaining a culture of compliance within your organization.

#### Before you begin

Role required: sn_grc_emp_user.grc_employee or sn_comp_case.compliance_case_business_user

#### Procedure

1. Navigate to **All** > **Self-Service** > **Employee Center**.
2. On the Employee Center landing page, select the **Risk & Compliance** tab.
3. In the Browse Risk & Compliance section, select **Report a Compliance Request**.
4. On the form, fill in the fields.

   For a description of the field values on the Report a Compliance Request form, see Raise a Compliance Request form.

5. Optional: On the Report a compliance request form, select **Add attachments** to attach supporting material or evidence.
6. Select **Submit**.

### Raise a Compliance Request form

Use the Raise a Compliance Request form in the Employee Center to raise a compliance request.

The following table lists the descriptions of the field values.

**Report a Compliance Request form**

| Field | Description |
|---|---|
| Name | Name of the request. For example, a request for the Policy Update - Annual medical |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Report a Compliance Request form (continued)**

| Field | Description |
|---|---|
| | examination is mandatory for all permanent employees. |
| Description | Brief description of the request. |
| Request type | Type of the request. |
| Priority | Priority of the request:<br>• **1 - Critical**<br>• **2- High**<br>• **3 - Moderate**<br>• **4 - Low**<br>• **5 - Planning** |
| Requested by | Name of the person who raised the request. |
| Requested on behalf of | Name of the person that you created the request for. |
| Business Unit | Business unit that is affected by the request. For example, Legal. |
| Location | Location where the request was raised. For example, Japan. |

### Create a compliance request in the Compliance Workspace

Raise a compliance request regarding organization's policies, inquiries, and guidelines by using the Compliance Case Management application. By seeking guidance, clarification, or approval, you contribute to maintaining a culture of compliance within the organization.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst and sn_compliance_ws.corporate_compliance_manager

#### Procedure

1. Navigate to **All** > **Compliance Workspace**.
2. Select the Compliance case management icon ( ).
3. On the Compliance Case Management landing page, select **Create**.
4. From the options available in the Create list, select **Request**.
5. On the form, fill in the fields.
   For a description of the field values on the Create a Compliance Case form, see Compliance request form.
6. Select **Save**.

### Compliance request form

Use the Create new compliance request form in the GRC: Compliance Case Management application to raise a compliance request.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following table lists the descriptions of the field values.

**Create new compliance request form**

| Field | Description |
|---|---|
| Number | Number of the request. This field is automatically set to a request number. |
| Name | Name of the request. For example, a request for the Policy Update - Annual medical examination is mandatory for all permanent employees. |
| Description | Brief description of the request. |
| Type | Type of the request. |
| State | Workflow state of the request. This field is automatically set to **New**. |
| Priority | Priority of the request:<br>• **None**<br>• **1 - Critical**<br>• **2- High**<br>• **3 - Moderate**<br>• **4 - Low**<br>• **5 - Planning** |
| Requested by | Name of the person who raised the request. |
| Requested on behalf of | Name of the person that you created the request for. |
| Assignment | |
| Assignment group | Group that is assigned to the request.<br>**Note:** The assignment group is preconfigured to the request type during the configuration setup. |
| Approvers | Person who should approve the request. |
| Assigned to | Person who is assigned to this request. |
| Watch list | User who must be informed about the request. |
| Primary origin | |
| Business unit | Business unit that is affected by the request. For example, Legal. |
| Location | Location where the request was raised. For example, Japan. |
| Schedule | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create new compliance request form (continued)**

| Field | Description |
|---|---|
| Created | Date when the request was raised. This field is automatically set to the current date and time. |
| Approved on | Date when the request was approved. |
| Activity | |
| Work notes (Private) | Notes or information about the request. |
| Additional comments (Customer visible) | Additional information about the request that you want to share with your customers. |

## Compliance case task workflow

You can collaborate with multiple teams to investigate, perform an impact assessment, and gather the evidence to capture the details and responses for review in the GRC: Compliance Case Management application.

After a compliance case is reported, the compliance analyst can create case tasks and assign those tasks to the various case task owners. The case task owners can then work on the tasks and submit them for the case analyst to review. There are three types of case tasks:

Assessment

An Assessment case task requires the case task owner to take an assessment and provide responses. A case task of this type can only be reassigned.

Investigation

An Investigation case task requires the case task owner to provide observations.

Others

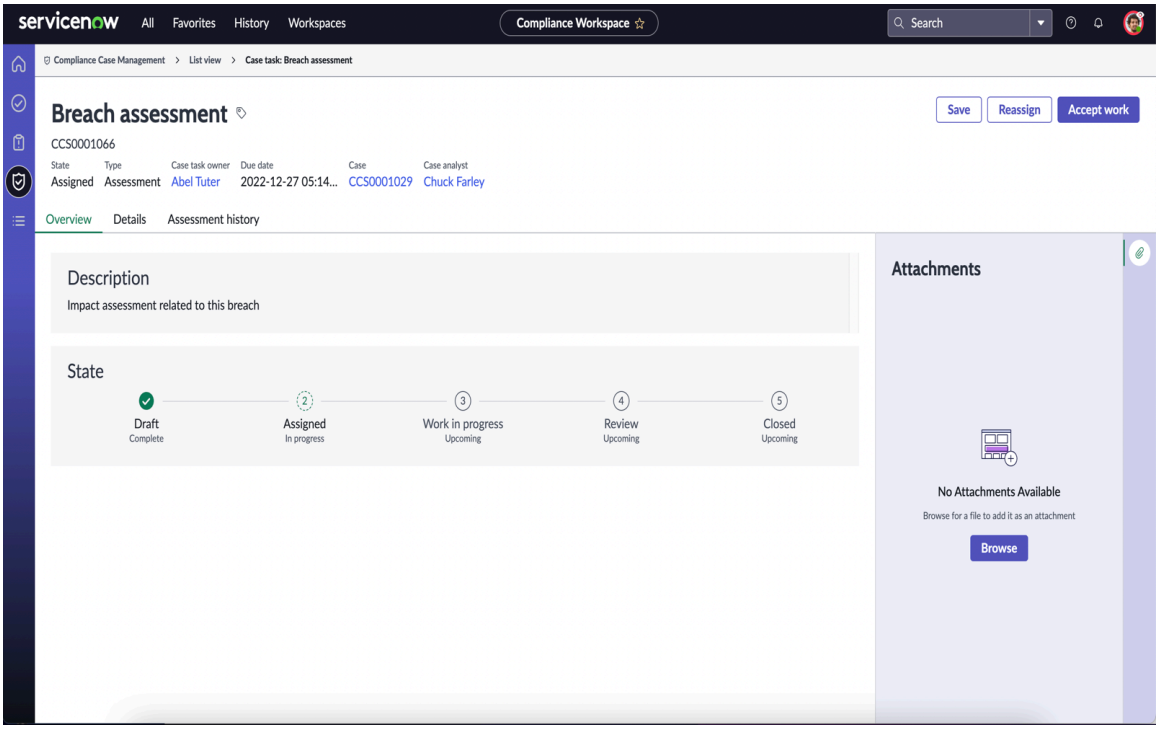
An Others case task also requires the case task owner to provide observations.

After the case task owners work on a task, they submit the task for the case analyst to review.

The following example displays the life cycle of a case task.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Case task workflow




## Create a case task

Create a case task to investigate, gather evidence, and perform an assessment so that you can analyze and assess a reported case in the GRC: Compliance Case Management application. Each case can have multiple case tasks that you can assign to different owners across multiple teams.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

### About this task

After a case is reported to the compliance team, a compliance case analyst can create case tasks and assign the tasks to the relevant task owners. This way, the compliance case analyst can collaborate with various teams to investigate, assess, and capture observations that are related to the case.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the list icon.
3. In the List section, select **All Cases**.
4. Open the case that you want to create a case task for.
5. Select the Case task related list.
6. Select **New**.
7. On the form, fill in the fields.

   For a description of the field values on the Case Task form, see Case task form.
8. Select **Save**.
9. To assign the task to the case task owner, select **Assign task**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. Optional: In the confirmation dialog box, provide your notes.
11. In the confirmation dialog box, select **Move to assigned**.
    The state of the record changes to **Assigned** and the case task is assigned to the case task owner.
12. Optional: To reassign the case task to another user before the case task is accepted by the case task owner that is specified by you, select **Reassign**.

    **Note:** You can only reassign the Assessment type of case tasks.

    a. In the **Assignment group** field, select the relevant group.
    b. In the **Case task owner** field, select a new owner.
    c. In the Reassign case task dialog box, select **Reassign**.

### Case task form

Use the Case Task form in the GRC: Compliance Case Management application to create a case task for a reported compliance case.

See the following table for a description of the field values.

#### Case task form

| Field | Description |
|---|---|
| Number | Number of the case task. This field is automatically set. |
| State | Workflow state of the case task. This field is automatically set to **Draft**. |
| Title | Name of the task that is being created for the case. For example, Investigation for wrongly charged late payment fees. |
| Type | Type of task:<br>• **Assessment**: Collect the responses from the users about the case.<br>**Note:** Only case tasks with the Assessment case task type can be reassigned to a different task owner if required.<br>• **Investigation**: Create a case task to perform any investigation for the case reported. For example, you may want to determine the cause of wrongly charged late payment fees.<br>• **Others**: Any other type of task that you configure. |
| Priority | Priority of the case task. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Case task form (continued)**

| Field | Description |
|---|---|
| Assessment template | Assessment template to assess the case. This field appears only when **Assessment** is selected from **Type**.<br><br>**Note:** Each case type can be mapped to specific assessment templates during the configuration. Only the templates that are mapped to the case are available for selection. For example, if the case type is **Financial fraud**, then the assessment templates that are specific to the financial fraud type are available for selection. You can't select the same assessment template if an open assessment with the selected assessment template is already being worked on. |
| Description | Brief description of the case task. This description is useful for the user who works on the case task. |
| Assignment | |
| Assignment group | Group that works on the case task. Any user who belongs to the selected group can work on the case task if a case task owner isn't specified. |
| Case task owner | Person who owns the case task. The user selected in this field must be a member from the assignment group. |
| Watch list | Users who must be informed about the case. |
| Schedule | |
| Due date | Date within which the case task must be completed.<br><br>**Note:** The due date must be before the date specified in the **Case closure SLA** field on the case form. |
| Accepted date | Date when the case is accepted. |
| Created | Date when the case is created and assigned to the case task owner. |
| Task closure date | Date when the task is closed. |
| Summary | |
| Observations | Observations that you make about the case while you're working on the case task. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Case task form (continued)**

| Field | Description |
|---|---|
| Activity | |
| Additional comments | Additional information about the case task. |

### Work on a case task

Accept the case task, provide the details requested by the case analyst, and submit the case task for a review in the GRC: Compliance Case Management application. When a case task is assigned to an assignment group, any user from the assignment group can accept and work on the task.

## Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

## About this task

If a case task is the Assessment type, the case task owner must take an assessment to determine the losses that were incurred from a case. In this case, the task owner can accept the work and then take the assessment. If the case task is the Investigation type or Others type, the case task owner can accept the task, provide observations, and submit the case for review to the case analyst.

## Procedure

1. Navigate to **Self Service** > **Employee Center**.
2. Access your task from the My Tasks module.
3. Open the task that is assigned to you.
4. In the Open section, select **Accept work**.
5. In the confirmation dialog box, select **Accept work**.
6. Depending on your case task type, select one of the following options.

| Choice | Steps |
|---|---|
| If the task is of type Assessment | **a.** Select **Take assessment**.<br>**b.** Respond to the questions in the assessment.<br>**c.** Select **Submit**.<br>**d.** Select **Save**. |
| If the task is of type Investigation or Others | **a.** In the **Observations** field, provide your comments.<br>**b.** Select **Save**.<br>**c.** Select **Ready for review**.<br>**d.** In the confirmation dialog box, provide your comments.<br>**e.** Select **Ready for review**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### What to do next

1. Add the areas that are impacted by a compliance case. For example, the impacted areas or objects that could be impacted are the entities, controls, locations, or users that are affected by the compliance case. For more information, see Add an impacted area to a compliance case.
2. Add the areas that are related to the compliance case. For example, the related areas include the policies, citations, control objectives, or risk events. For more information, see Add a related area to a compliance case.
3. Add the causes and consequences of this compliance case. For example, you can add the root cause for the reported compliance case or event and its consequences on the organization. For more information, see Add a cause and consequence to a compliance case.
4. Add the compliance regulations that might be impacted to the compliance case. For more information, see Add compliance regulations to a compliance case.
5. Add or create an issue related to a compliance case. For more information, see Add or create an issue for a compliance case.

## Reassign an Assessment type case task

Reassign an Assessment type case task to another user in the GRC: Compliance Case Management application. For example, a case analyst or a case task owner can reassign a compliance case task to another case task owner if a case task is wrongly assigned or isn't accepted by the case task owner.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

### About this task

As a case analyst, after a task is assigned to a case task owner, you can reassign the task to another user.

As a case task owner, you can also accept the task, start working on it, and then reassign the partially completed task to another user. When you reassign a partially completed case task to another user, the data that you provide also gets copied and is available to the new case task owner. The newly assigned task owner can modify the case task based on that owner's requirements.

**Note:** You can only reassign the case tasks that have the **Type** field set to **Assessment**.

### Procedure

1. Navigate to **Self Service** > **Employee Center**.
2. Access your task from the My tasks module.
3. Open the task that you want to work on.
4. In the Open section, select **Reassign**.
   The Reassign case task dialog box appears.
5. In the **Assignment group** field, select the assignment group.
6. In the **Case task owner** field, select the owner.
7. In the Reassign case task dialog box, select **Reassign**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Review and close a case task

Review and close a case task after a case task owner provides responses and observations for the case in the GRC: Compliance Case Management application.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Tasks module, open the task to review.
3. Review the case task and then select one of the following options.

| Choice | Steps |
|---|---|
| To request revision of the details provided by the case task owner | **a.** Select **Request revision**.<br>**b.** Provide your notes and comments.<br>**c.** Select **Request revision**. |
| To close the task as complete | **a.** Select **Complete**.<br>**b.** Provide your notes and comments.<br>**c.** Select **Close as complete**. |
| To close the task as incomplete | **a.** Select **Close as incomplete**.<br>**b.** Provide your notes and comments.<br>**c.** Select **Close as incomplete**. |
| To cancel the case task | **a.** Select **Cancel**.<br>**b.** Provide your notes and comments.<br>**c.** Select **Cancel**. |

## Add an impacted area to a compliance case

Add an impacted area or object that is affected by the compliance case or event in the GRC: Compliance Case Management application.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

#### About this task

You can specify the impacted areas or objects, such as the entities, controls, companies, and users that are affected by the compliance case. A compliance administrator can also configure the options for the impacted areas in the application setup.

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the list  icon.
3. From the list, select **All Cases**.
4. Open the case that you want to add an impacted area in.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Select the Impacted areas related list.
6. Select **Add**.
7. Select the impacted area type.
   Records related to the selected record type are available for your selection.
8. Select the records from the available list.
   Modifying the **Select type** field clears the current selection.
9. Select **Add**.
10. Select **Save**.

## Add a related area to a compliance case

Add an area that is related to the compliance case or event that is reported in the GRC: Compliance Case Management application.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

### About this task

You can specify the related areas for a compliance case or reported event. Related areas include the policies, citations, control objectives, control, and risk events. A compliance administrator can also configure the options for the related areas in the application setup.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the list  icon.
3. From the list, select **All Cases**.
4. Open the case that you want to add a related area to.
5. Select the Related areas related list.
6. Select **Add**.
7. Select the related area type.
   Records related to the selected record type are available for your selection.
8. Select the records from the available list.
   Modifying the **Select type** field clears the current selection.
9. Select **Add**.
10. Select **Save**.

## Add a cause and consequence to a compliance case

Define the root cause for the reported compliance case or event and its consequences on the organization by using the GRC: Compliance Case Management application.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

### About this task

You can add multiple causes to a compliance case or event and define a primary cause. Any compliance case can have only one primary cause. You can also add a cause that is suspected but not confirmed. The Compliance Case Management application enables you

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

to add the consequences based on the reported case and any action or remediation plan that is in place.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the list  icon.
3. From the list, select **All Cases**.
4. Open the case that you want to add a cause and consequence to.
5. Select **New**.
6. On the form, fill in the fields.
   For a description of the field values on the Cause and Consequence form, see Cause and Consequence form.
7. Select **Save**.

#### Cause and Consequence form

Use the Cause and Consequence form to define the cause and consequence that a case has on your organization in the GRC: Compliance Case Management application.

See the following table for a description of the field values.

**Cause and Consequence form**

| Field | Description |
|---|---|
| Cause | Cause for the case or event. |
| Cause status | Status of the cause:<br>• **Suspected**: When the cause isn't confirmed.<br>• **Confirmed**: When the cause is confirmed. |
| Primary cause | Option to select the cause as the primary cause. |
| Cause description | Brief description of the cause. |
| Consequences and actions | |
| Consequences | Consequences of the case or event. You can select multiple consequences for a reported case. |
| Actions taken | Any action or measures taken to address the case. |
| Summary | |
| Observations | Overall observations, if any. |

## Add compliance regulations to a compliance case

Add the regulations that are or can be impacted by the reported compliance case. In the ServiceNow platform, regulations are captured as authority documents. Adding the

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

regulations to the case enables you to identify which regulations are breached or violated and prevents your organization from getting penalties or fines for this case.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

### About this task

As a case analyst, you can choose and add the regulations that are related to the reported case. By default, all the regulations in the system are displayed. After you add the regulations, you must analyze which regulations have been violated and set their reporting status. The reporting status helps you to determine if the regulation must be reported or not.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the list  icon.
3. From the list, select **All Cases**.
4. Open the case that you want to add a regulation to.
5. Select the Regulations related list and do the following actions:
   a. Select **Add**.
   b. Select the regulations to add.
   c. Select **Add**.
6. To set the reporting status of a regulation, select and open the regulation.
7. On the form, fill in the fields.

**Regulation form**

| Field | Description |
|---|---|
| Case | Case that you're adding the regulation to. This field is automatically set to the case name. |
| Reporting status | Status to determine if the regulation must be reported immediately, in the future, or doesn't need to be reported at all. The options are as follows:<br>◦ **To be determined**: When you're not sure if the violation must be reported.<br>◦ **Reportable**: When the violation must be reported.<br>◦ **Non-reportable**: When the violation doesn't need to be reported.<br>◦ **Potentially reportable**: When the violation can be reported in the future based on the case investigation. |
| Authority document | Authority document that forms the regulation. |
| Lodgement date | Date that the regulation is reported to the regulators. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Description | Brief description of the regulation violation based on your analysis. |

8. Select **Save**.

## Add or create an issue for a compliance case

Identify and add an issue that is related to the impacted areas of a reported compliance case. You can also create an issue from the GRC: Compliance Case Management landing page.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the list  icon.
3. From the list, select **All Cases**.
4. Open the case that you want to add an issue to and then select one of the following options.

| Option | Action |
|---|---|
| To add an existing issue | **a.** Select **Add**<br>**b.** Select the issues that you want to add.<br>**c.** Select **Add**. |
| To create an issue | See the Create an Issue form. |

5. Select **Save**.

### Create an Issue form

Use the Create an Issue form in GRC: Compliance Case Management to add an issue to a compliance case.

For a description of the field values, see the following table.

#### Create an Issue form

| Field | Description |
|---|---|
| Issue | |
| Number | Number of the issue. This field is automatically filled in. |
| Name | Name of the issue. |
| Issue source | Source of the issue, such as Business service or Scenario analysis. This field is automatically filled in. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create an Issue form (continued)**

| Field | Description |
|---|---|
| Issue type | Source from where the issue was created. This field is automatically filled with one of the following options based on how the issue was created:<br>• Control design effectiveness failure<br>• Control operative effectiveness failure<br>• Control doesn't meet requirement<br>• Control doesn't exist<br>• Non-compliance to a regulation<br>• Non-compliance to a policy<br>• Improvement or suggestion to an existing policy<br>• Recommendation for a new policy<br>• Process optimization or improvement<br>• Observation<br>• Data breach<br>• Fraud<br>• Misstatement<br>• Training<br>• Documentation |
| Classification | Classification of the issue. This field is automatically filled in with one of the following options:<br>• Audit<br>• Compliance<br>• Operational Resilience<br>• Risk<br>• Vendor |
| Location | Location of the issue. |
| State | State of the issue:<br>• **New**<br>• **Analyze**<br>• **Respond**<br>• **Review**<br>• **Closed Complete**<br>• **Closed Incomplete** |
| Substate | Substate of the issue. This field is automatically filled in. |
| Priority | Priority of the issue: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create an Issue form (continued)**

| Field | Description |
|---|---|
| | • **Critical**<br>• **High**<br>• **Moderate**<br>• **Low**<br>• **Planning** |
| Issue rating | Rating of the issue:<br>• **Very High**<br>• **High**<br>• **Moderate**<br>• **Low**<br>• **Very Low** |
| Description | Approver of the scenario analysis plan. |
| Assignment | |
| Assignment group | Assignment group for the issue. For example, Application Development group. |
| Assigned to | User that the issue is assigned to. |
| Issue manager group | Manager group that the issue is assigned to:<br>• **Compliance Managers**<br>• **IT Risk Managers**<br>• **Risk Managers** |
| Issue manager | Manager that the issue is assigned to. |
| Watchlist | Users who are on the watchlist for the issue. |
| Schedule | |
| Due date | Date when the issue is due. |
| Confirmed date | Confirmation date for the issue. This field is automatically filled in. |
| Planned start date | Planned start date for the issue. |
| Planned end date | Planned end date for the issue. |
| Duration | Duration for the issue in days, hours, minutes, and seconds. |
| Created | Date on which the issue is created. This field is automatically filled in. |
| Closed | Date on which the issue is closed. |
| Actual start date | Actual start date for the issue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create an Issue form (continued)**

| Field | Description |
|---|---|
| Actual end date | Actual end date for the issue. |
| Actual duration | Actual duration for the issue in days, hours, minutes, and seconds. |
| Issue grouping | |
| Parent issue | Parent issue that is associated with the issue. |
| Issue group rule | Group rule for the issue. This field is automatically filled in. |
| Action plan | |
| Recommendation | Recommendation for the issue. |
| Action plan | Action plan for the issue. |
| Activity | |
| Work notes | Work notes for the issue. |
| Additional comments | Additional comments for the issue. |
| Settings | |
| Functional domain | Functional domain for the issue. |

## Compose emails in GRC: Compliance Case Management

Compose and send an email for compliance cases and requests using the GRC: Compliance Case Management application. This feature helps you to communicate with different stakeholders within or outside your organization.

### Before you begin

Role required: sn_grc_case_mgmt.grc_case_analyst

### About this task

You can compose and send emails regarding your cases and requests to multiple stakeholders. For example, you can consult the legal team for any obligatory opinions and suggestions on the recorded compliance case. You can manage the emails from the case or request record page.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the list  icon.
3. To compose an email for a compliance case, select **All cases**.
4. To compose an email for a compliance request, select **All requests**.
5. Open the compliance case or compliance request that you want to export as a PDF report.
6. Select the More actions  icon.
7. Select **Compose Email**.
8. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Email Draft form**

| Field | Description |
|---|---|
| To | Email id of the recipient. You can add multiple email ids in this field to send email to more than one recipient. |
| Subject | A brief summary or title of your email. |
| Email message | Body of your message includes any information, requests, or details you want to convey to the recipient. You can format the text, add attachments, and include links in this section.<br><br>**Note:** You can send emails to both ServiceNow® users and external stakeholders who don't have access to the ServiceNow® instance. You must provide the basic record details in the subject line or body of the email to make them aware of the record you're referring to. |

9. Optional: To add attachments, select **Attach File**.
10. Select **Send Email**.

## Export a report to PDF

Create Portable Document Format (PDF) reports for compliance cases or requests using predefined or customized templates in the GRC: Compliance Case Management application. This feature enables the stakeholders who may not have access to the application can still access the data.

### Before you begin

Role required: sn_comp_case.compliance_case_analyst

### About this task

You can export compliance data to PDF reports for easy sharing with audit teams, partners, or internal committees, eliminating the requirement for application access. A compliance administrator can select a predefined template or create a customized document template to generate reports. For more information, see Configure a PDF document template.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the list icon.
3. To generate a compliance case report, select **All cases**.
4. To generate a compliance request report, select **All requests**.
5. Open the compliance case or compliance request that you want to export as a PDF report.
6. Select the More actions icon.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Select **Export PDF**.
   The **Export PDF** button appears only when a document template is specified in the record type.
8. Select the template to generate a PDF report.
9. Select **Export**.
   A PDF report is generated and is available in the Attachments section of the record to download.
10. To download a local copy of the PDF report, select the More actions icon on the PDF report, and select **Download**.

## Compliance Case Management reference

Reference topics provide additional information such as the tables and roles that are installed with the GRC: Compliance Case Management application.

### Tables installed with Compliance Case Management

Tables are added with the activation of the GRC: Compliance Case Management application.

See the following table for a description of the tables that were added with the GRC: Compliance Case Management application.

**Tables installed**

| Table | Description |
|---|---|
| GRC case<br>[sn_grc_case_mgmt_case] | Stores all the compliance case details. |
| Case classification<br>[sn_grc_case_mgmt_case_classification] | Stores the compliance case classifications. |
| Case task<br>[sn_grc_case_mgmt_case_task] | Stores all the case tasks that were created for the compliance case. |
| Case type<br>[sn_grc_case_mgmt_case_type] | Stores the case type and case subtype details. |
| Cause<br>[sn_grc_case_mgmt_cause] | Stores the causes that were added to the library and mapped to the case. |
| Cause and consequence<br>[sn_grc_case_mgmt_cause_consequence] | Stores the causes and consequences that were mapped to the case. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tables installed (continued)**

| Table | Description |
|---|---|
| Consequence<br><br>[sn_grc_case_mgmt_consequence] | Stores the consequences that were added to the library and mapped to the case. |
| GRC core case<br><br>[sn_grc_case_mgmt_core_case] | Stores the core functionality details of the case. |
| Impacted area<br><br>[sn_grc_case_mgmt_impacted_area] | Stores the impacted areas that were mapped to the case. |
| Case task to assessment instance<br><br>[sn_grc_case_mgmt_m2m_case_task_asmt_instance] | Stores the assessment details on the case tasks of the type assessment. |
| Issue to case<br><br>[sn_grc_case_mgmt_m2m_issue_case] | Stores the issues that were mapped to the case. |
| Regulation<br><br>[sn_grc_case_mgmt_regulation] | Stores the regulations that were mapped to the case. |
| Regulated area<br><br>[sn_grc_case_mgmt_related_area] | Stores the related areas that were mapped to the case. |
| Compliance case<br><br>[sn_comp_case_compliance_case] | Stores the compliance case records. |

## Roles installed with Compliance Case Management

The GRC: Compliance Case Management installs the roles for the compliance analyst, the compliance manager, and the compliance administrator to perform their respective tasks.

**Roles and their descriptions**

| Role title [name] | Description | Contains roles |
|---|---|---|
| Compliance Case Business User<br><br>[sn_comp_case.compliance_case_business_user] | The compliance case business user can perform the following tasks: | sn_grc_case_mgmt.grc_case_business_user |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles and their descriptions (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| | • Create compliance cases and requests from the Employee Center<br>• Work on the case tasks.<br>. | |
| Compliance Case Analyst<br><br>[sn_comp_case.compliance_case_analyst] | Compliance case analyst can review the case. The compliance case analyst can perform the following tasks:<br>• Review the key stakeholders, impacted areas, related areas, causes and consequences, regulations, and issues that are assigned to the case analyst.<br>• Review any unassigned cases. | • sn_grc_case_mgmt.grc_case_analyst<br>• sn_comp_case.compliance_case_business_user |
| Compliance Case Manager<br><br>[sn_comp_case.compliance_case_manager] | Compliance case manager can review and work on the created cases. The compliance case manager can perform the following tasks:<br>• Review the key stakeholders, impacted areas, related areas, causes and consequences, regulations, and issues that are assigned to the case analyst.<br>• Review all cases. | • sn_comp_case.compliance_case_analyst<br>• sn_grc_case_mgmt.grc_case_manager |
| Compliance Case Admin<br><br>[sn_comp_case.compliance_case_admin] | Compliance case administrators can configure the Compliance Case Management application. They can perform the following tasks:<br>• Create a case type.<br>• Create a state model and transitions. | • sn_grc_case_mgmt.grc_case_admin<br>• sn_comp_case.compliance_case_manager |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles and their descriptions (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| | • Create an assessment template.<br>• Delete cases.<br>• Review the key stakeholders, impacted areas, related areas, causes and consequences, regulations, and issues that are assigned to the case analyst. | |
| GRC Employee User<br><br>[sn_grc_emp_user.grc_employee] | GRC employee users can create compliance cases and requests from the Employee Center. | NA |

# Continuous Authorization and Monitoring

Continuous Authorization and Monitoring employs the seven steps defined by the RMF to allow you to make better-informed decisions about your security posture.

## Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

The Continuous Authorization and Monitoring (com.sn_irm_cont_auth_monitor) plugin is available as a separate subscription and requires activation.

| | | |
|---|---|---|
| **Explore**<br>Continuous Authorization & Monitoring | **Set up**<br>• Download Continuous Authorization and Monitoring<br>• Assign Continuous Authorization and Monitoring roles to your users | **Administer**<br>Prepare the authorization package |
| **Use**<br>• Categorize the authorization package<br>• Select controls for an authorization package | **Develop**<br>• [redacted]<br>• Developer documentation [redacted] | **Troubleshoot and get help**<br>• Ask or answer questions in the Continuous Authorization and Monitoring forum on the ServiceNow Community |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| | | |
|---|---|---|
| • Implement controls<br>• Assess, authorize, monitor, and generate reports | | • Search the Known Error Por-<br>• Contact Customer Service |

## Understanding Continuous Authorization and Monitoring

The ServiceNow® Continuous Authorization and Monitoring application (CAM for short) applies a standardized approach to automating NIST's Risk Management Framework (RMF).

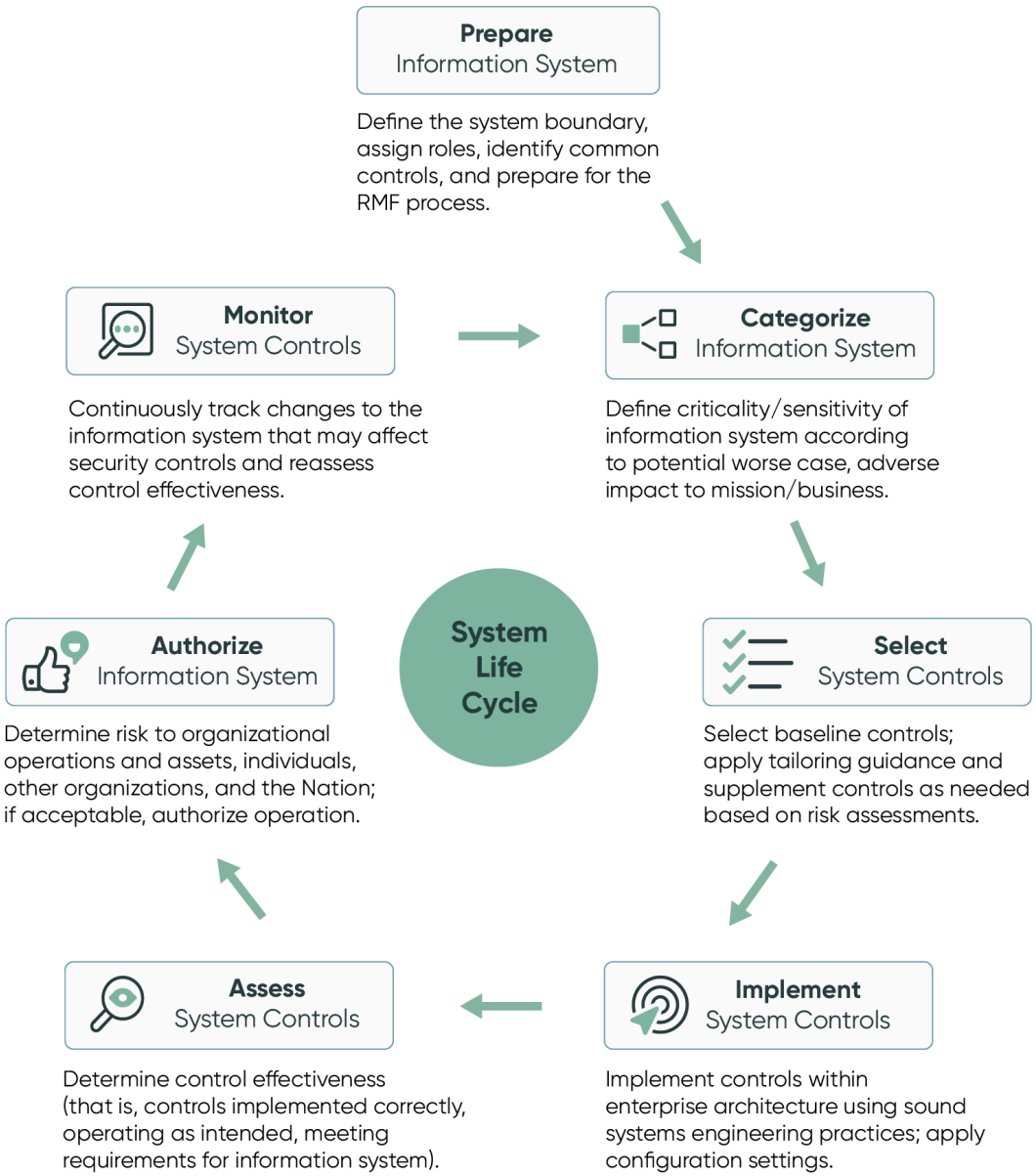
RMF was mandated by the U.S. Federal government to provide the necessary resiliency to support the economic and national security interests of the United States. Continuous Authorization and Monitoring employs the seven steps defined by the RMF to allow you to make better-informed decisions about your security posture.

### The life cycle as defined by the RMF

RMF consists of the seven steps illustrated here.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**RMF security life cycle**




## Continuous Authorization and Monitoring implementation

Use the steps in the Continuous Authorization and Monitoring application checklist to download Continuous Authorization and Monitoring from the ServiceNow Store, and get it ready for operation.

### Setup checklist for Continuous Authorization and Monitoring

This checklist includes the setup tasks that you are required to complete in your Now Platform® instance. When you have completed these tasks, the base system is ready for operation.

**Before you begin**
Role required: admin, sn_irm_cont_auth.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Create and print a PDF of this checklist topic and check off tasks as you complete them.
2. To generate a PDF, click the **Save As PDF** icon ( ) at the top of the topic and click **Selected topic**.

**Continuous Authorization and Monitoring application checklist**

| Item | Description |
|---|---|
| ☐ | As a user with the System Administrator role, verify that you have the GRC core applications installed on a Now Platform instance.<br><br>**Note:** The GRC applications and the Now Platform instance should be from the same family release.<br><br>**a.** To verify the GRC: GRC Profile application is installed on your instance, navigate to **Plugins** and search for GRC Profile.<br>**b.** If the GRC Profile core application is not already installed, click **Install** to install it.<br>**c.** Also install the following applications, as needed:<br>▪ GRC: Policy and Compliance Management<br>▪ GRC: Risk Management<br>▪ GRC: Audit Management<br>**d.** After these applications have been installed, install the Continuous Authorization and Monitoring core application.<br><br>If the applications mentioned above are not visible in your instance, all of the GRC core applications are available from the ServiceNow Store. For more information about getting entitlement, downloading, and installing the GRC core applications, see GRC and the ServiceNow Store. |
| ☐ | As a user with the Continuous Authorization and Monitoring Administrator role, in your Now Platform instance, verify that you have assigned users with the required Now Platform roles.<br><br>For detailed instructions and a list of Continuous Authorization and Monitoring roles, see Assign Continuous Authorization and Monitoring roles to your users. |

Congratulations! You have successfully set up the Continuous Authorization and Monitoring base system. Many of the elements included in the base system can be customized for your particular business needs. Refer to the links in the checklist for more information.

## Download Continuous Authorization and Monitoring

Before you run GRC: Continuous Authorization and Monitoring (com.sn_irm_cont_auth_monitor) in your instance, you must download it from the ServiceNow Store.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: admin

### Procedure

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

Related topics

List of plugins

## Assign Continuous Authorization and Monitoring roles to your users

Before you can successfully implement or use the Continuous Authorization and Monitoring application, you must assign roles to your users.

### Before you begin
Role required: admin

### Procedure

1. Navigate to **All** > **User Administration** > **Users**.
2. Select the name of a user.
3. Select the **Roles** tab.
4. Select **Edit**.
5. Move the roles that you want to assign to the user from the Collection side to the Roles List, then select **Save**.
6. Repeat these steps for each of your users.

| Role title [name] | Description |
|---|---|
| Authorization Official<br><br>[sn_irm_cont_auth.authorization_official] | The Authorization Official is responsible for accepting an information system into an operational environment at a known risk level.<br><br>The Authorization Official role contains:<br>◦ sn_audit.user<br>◦ sn_compliance.user<br>◦ sn_irm_cont_auth.reader |
| Continuous Authorization and Monitoring administrator<br><br>[sn_irm_cont_auth.admin] | The Continuous Authorization and Monitoring administrator is responsible for all system administration duties in the Continuous Authorization and Monitoring application.<br><br>The Continuous Authorization and Monitoring administrator role contains:<br>◦ sn_audit.manager<br>◦ sn_compliance.admin<br>◦ sn_doc.admin |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role title [name] | Description |
| --- | --- |
| | ◦ sn_irm_cont_auth.reader<br>◦ sn_irm_cont_auth.scheduler |
| Executive Reader<br>[sn_irm_cont_auth.executive_read] | The Executive Reader has read-only access to all modules of the Continuous Authorization and Monitoring application.<br>The Executive Reader role contains: sn_irm_cont_auth.reader. |
| Information Owner<br>[sn_irm_cont_auth.information_owner] | The Information Owner is responsible for statutory, management, or operational authority and the establishment of policies and procedures governing its generation, collection, processing, dissemination, and disposal.<br>The Information Owner role contains: sn_irm_cont_auth.reader. |
| Information System Security Manager<br>[sn_irm_cont_auth.info_system_sec_manager] | Responsible for conducting information system security management activities. They develop and maintain the system-level cybersecurity program. |
| Information System Security Officer<br>[sn_irm_cont_auth.info_system_sec_officer] | Responsible for ensuring that the appropriate operational security posture is maintained for an information system.<br>The Information System Security Officer role contains:<br>◦ sn_audit.user<br>◦ sn_compliance.user<br>◦ sn_grc.user<br>◦ sn_irm_cont_auth.reader |
| Reader<br>[sn_irm_cont_auth.reader] | The Reader is a read-only role.<br>The Reader role contains:<br>◦ sn_compliance.reader<br>◦ sn_incident_read<br>◦ sn_change_read |
| Scheduler<br>[sn_irm_cont_auth.scheduler] | The Scheduler is responsible for running all scheduled jobs for the application. This role is for a technical user.<br>The Scheduler role contains: sn_irm_cont_auth..system_owner. |
| Security Control Assessor<br>[sn_irm_cont_auth.sec_control_assessor] | The Security Control Assessor (SCA) is responsible for conducting a thorough assessment of the management, |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role title [name] | Description |
|---|---|
| | operational, and technical security controls of an information system.<br><br>The Security Control Assessor role contains:<br>◦ sn_audit.manager<br>◦ sn_compliance.user<br>◦ sn_irm_cont_auth.reader |
| System Owner<br><br>[sn_irm_cont_auth.system_owner] | The System Owner is responsible for procuring, developing, integrating, modifying, operating, and maintaining an information system.<br><br>The System Owner role contains:<br>◦ sn_audit.user<br>◦ sn_compliance.user<br>◦ sn_irm_cont_auth.reader |
| System User<br><br>[sn_irm_cont_auth.system_user] | The System User is responsible for performing actual work in the system.<br><br>The System User role contains: sn_irm_cont_auth.reader. |

## Prepare the authorization package

The first RMF-mandated step in CAM is Prepare. In this step, you can set up authorization boundaries, control overlays, and information types, as well as create the actual authorization package.

When the Prepare step has been completed, the subsequent six steps cycle over and over to ensure continuous authorization and monitoring of controls.

### Define authorization boundaries

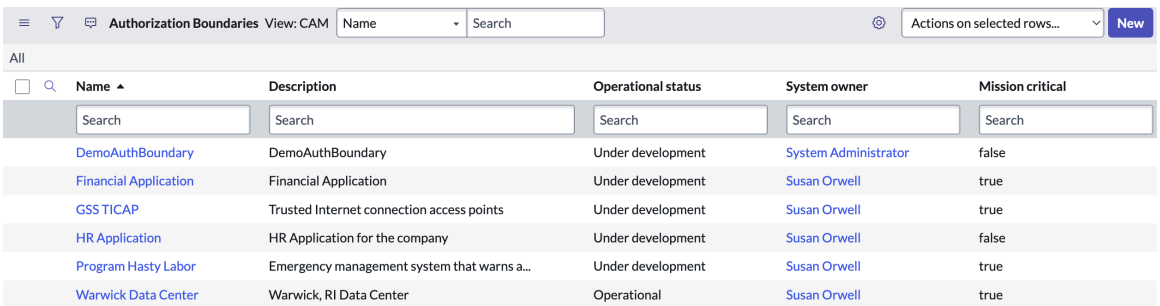
An authorization boundary defines the scope of a particular system that can be continuously managed and monitored using the CAM application.

#### Before you begin

Role required: sn_irm_cont_auth.system_owner or sn_irm_cont_auth.admin

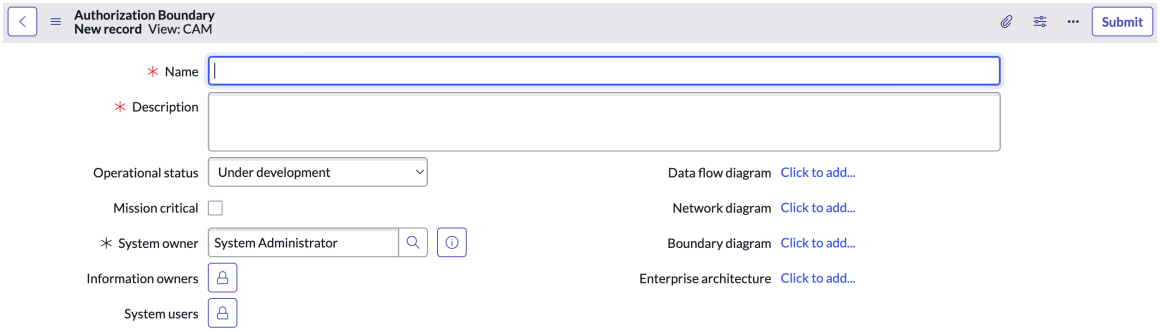
#### Procedure

1. Navigate to **All** > **Continuous Authorization & Monitoring** > **All Authorization Boundaries**.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Click **New**.




3. On the form, fill in the fields.

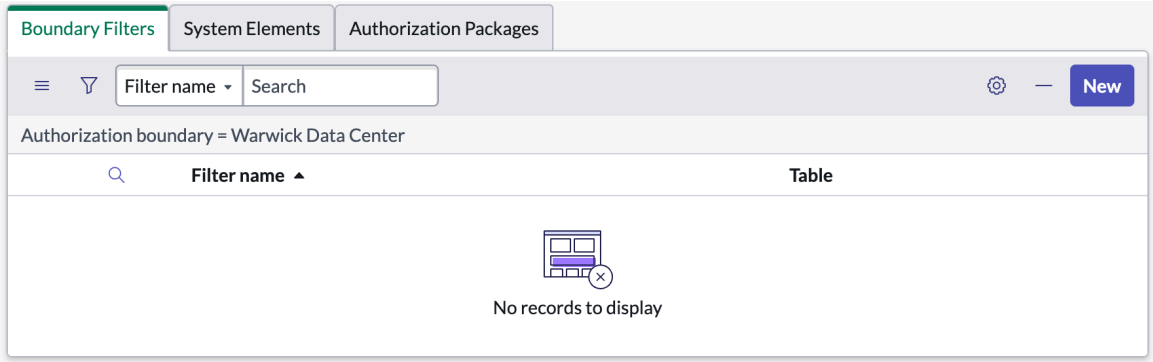
**Authorization Boundary**

| Field | Description |
|---|---|
| Name | A name for this boundary. |
| Description | A description for this boundary. |
| Operational status | The operational status:<br>◦ Under development<br>◦ Reauthorize<br>◦ Operational<br>◦ Decommissioned |
| Mission critical | The boundary is mission critical if selected. |
| System owner | The individual responsible for procuring, developing, integrating, modifying, operating, and maintaining an information system. |
| Information owners | The individuals responsible for statutory, management, and operational authority. |
| System users | The users responsible for performing the actual work on the system. |
| Diagrams | If needed, or if you do not have a CMDB, add data flow, network, and boundary diagrams. |

4. Save the record.

The following tabs appear. Use these tabs to identify what systems and parts of systems you own and should go through the authorization process.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




5. You can use the **Boundary Filters** tab to create filters for identifying all of your system elements.
   After running the filters, the results appear in the **System Elements** tab.
6. If elements appear that should not be included in the authorization process, you can select them, and select **Delete** from the **Actions on selected rows** list at the bottom of the screen.
7. You can click **Add** to include additional assets or systems to the list of system elements in the authorization boundary.

### What to do next

This completes the procedure for defining your authorization boundary. The next step is to create the authorization package that will be processed through approvals. You can initiate the process by clicking the **Authorization Packages** tab or via the navigation pane. For details, see Create an authorization package.

## Create an authorization package

After you have defined the authorization boundaries for the assets or systems that you want to send through the Authorization to Operate process, you must create an authorization package for that purpose. The package is then processed through the seven steps mandated by the RMF.

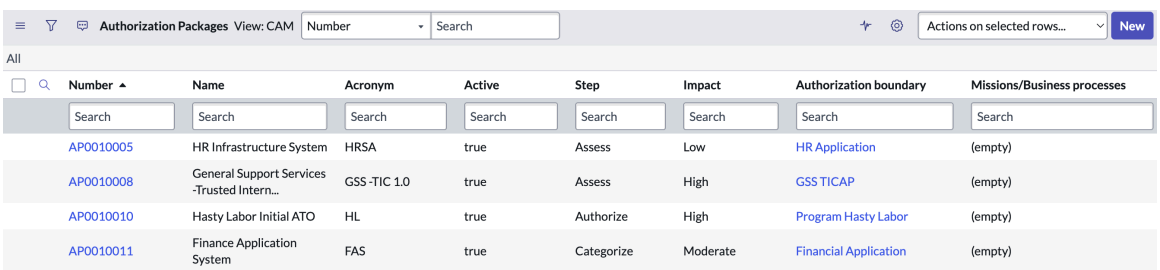
### Before you begin

Role required: sn_irm_cont_auth.system_owner or sn_irm_cont_auth.admin

**Note:** These roles are required for accessing the authorization package only after it has transitioned beyond the Prepare state.

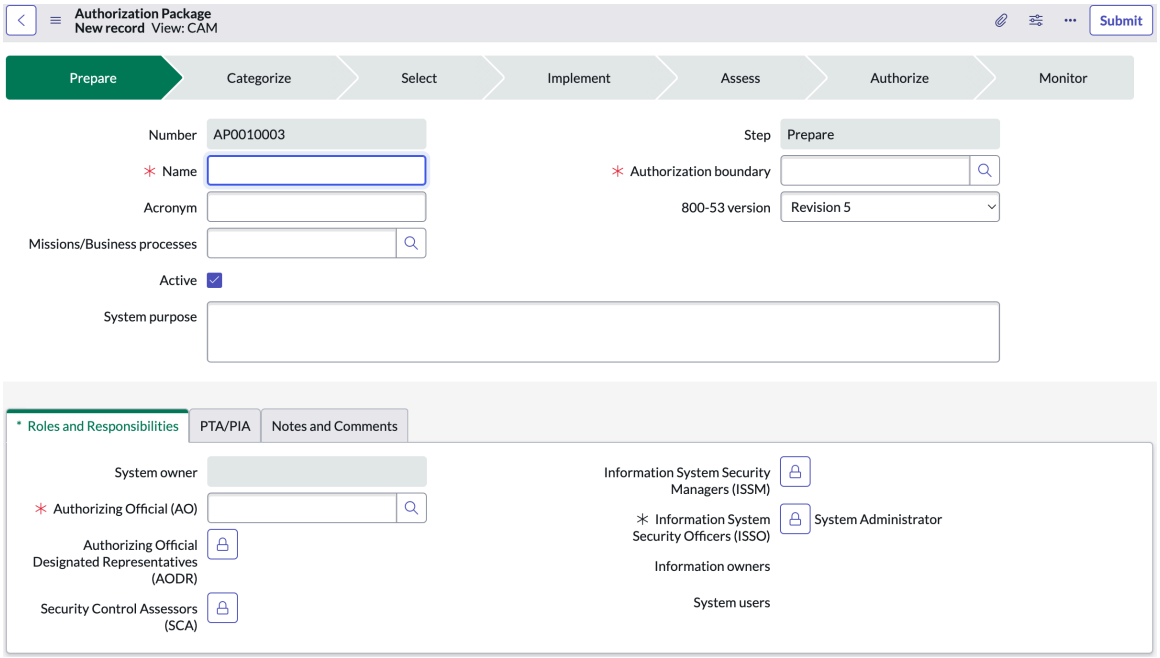
### Procedure

1. Navigate to **All** > **Continuous Authorization & Monitoring** > **All Authorization Packages**.




2. Click **New**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. On the form, fill in the fields.

### Authorization Package form

| Field | Description |
|---|---|
| Number | Auto-generated Authorization Package number. |
| Name | A name for the package. |
| Acronym | If needed, an acronym for identifying the package. |
| Missions/ Business processes | The appropriate business process for this authorization package. Business processes are defined on the Now Platform; for example, at **Policy & Compliance** > **Scoping** > **Business Processes**. |
| Active | Activate the authorization package. |
| Step | The RMF step currently assigned to the package. |
| Authorization boundary | The authorization boundary for this package. |
| System purpose | The purpose behind this authorization package. |

4. Click the **Roles and Responsibilities** tab and define the roles of various stakeholders during the review and approval process.

### Roles and Responsibilities tab

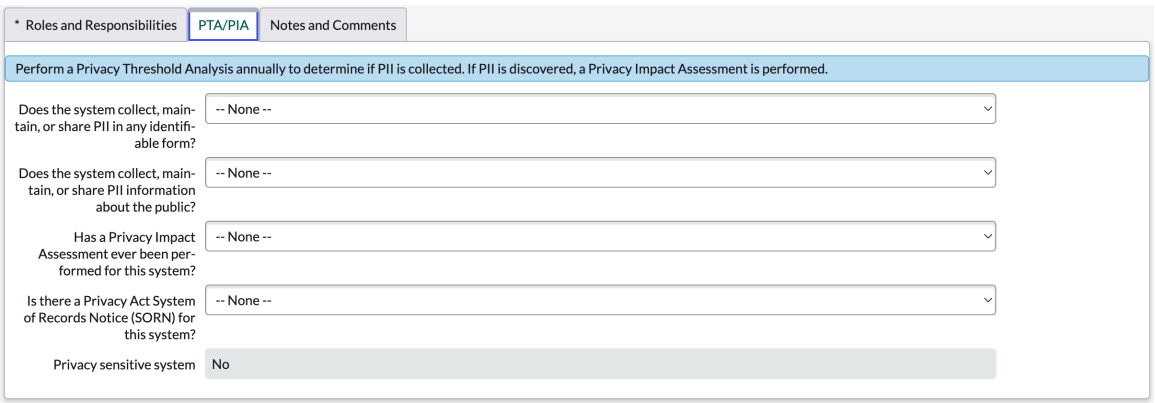
| Field | Description |
|---|---|
| System owner | The individual responsible for procuring, developing, integrating, modifying, operating, and maintaining an information system. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Authorizing Official (AO) | The individual responsible for accepting an information system into an operational environment at a known risk level. Typically, this person is at the CISO or deputy CISO level. |
| Authorizing Official Designated Representatives (AODR) | One or more AODRs. |
| Security Control Assessors (SCA) | The individuals responsible for conducting a thorough assessment of the controls of an information system. |
| Information System Security Managers (ISSM) | The individuals responsible for conducting information system security management activities as designated by the ISSO. |
| Information System Security Officers (ISSO) | The individuals responsible for ensuring that the appropriate operational security posture is maintained for an information system. |
| Information owners | The individuals responsible for statutory, management, and operational authority. |
| System users | The users responsible for performing the actual work on the system. |

5. Click the **PTA/PIA** tab and perform the Privacy Threshold Analysis by answering the questions.

   The PTA identifies whether various types of the Personal Identifiable Information (PII) exist in the systems being authorized.




6. If you answered **No** to all of the questions, you are not required to take a Privacy Impact Analysis and can click **Submit**.
7. If you answered **Yes** to any of the questions, you must take a Privacy Impact Analysis.

   a. In the Assessment respondents field, click the lock icon and select the users you want to take the assessment.

   b. When you have selected the respondents, click the lock icon again.

   c. Click **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The assessment request notification is sent to the selected respondents.

**d.** When the PIA has been completed, the assessment responses appear in a related list in the Authorization Package form.

**8.** Click the **Notes and Comments** tab to add any customer-facing notes to the package.

**9.** Click **Categorize** to transition the package to the next step

## Categorize the authorization package

In the Categorize step, you define the criticality or sensitivity of your information system according to potential worst-case scenarios. This involves selecting information types for the package from a list of information types provided by NIST and using the information types to define the impact levels for the package.

### Before you begin

Role required: to use the Categorize button:

- sn_irm_cont_auth.system_owner
- sn_irm_cont_auth.info_system_sec_manager
- sn_irm_cont_auth.info_system_sec_officer

Role required: to write to an authorization package:

- sn_irm_cont_auth.admin
- sn_irm_cont_auth.system_owner
- sn_irm_cont_auth.info_system_sec_manager
- sn_irm_cont_auth.authorization_official
- sn_irm_cont_auth.info_system_sec_officer

Role required: to select information types:

- sn_irm_cont_auth.admin
- sn_irm_cont_auth.system_owner

Role required: to write to overridden fields on the Package form:

- sn_irm_cont_auth.system_owner

### About this task

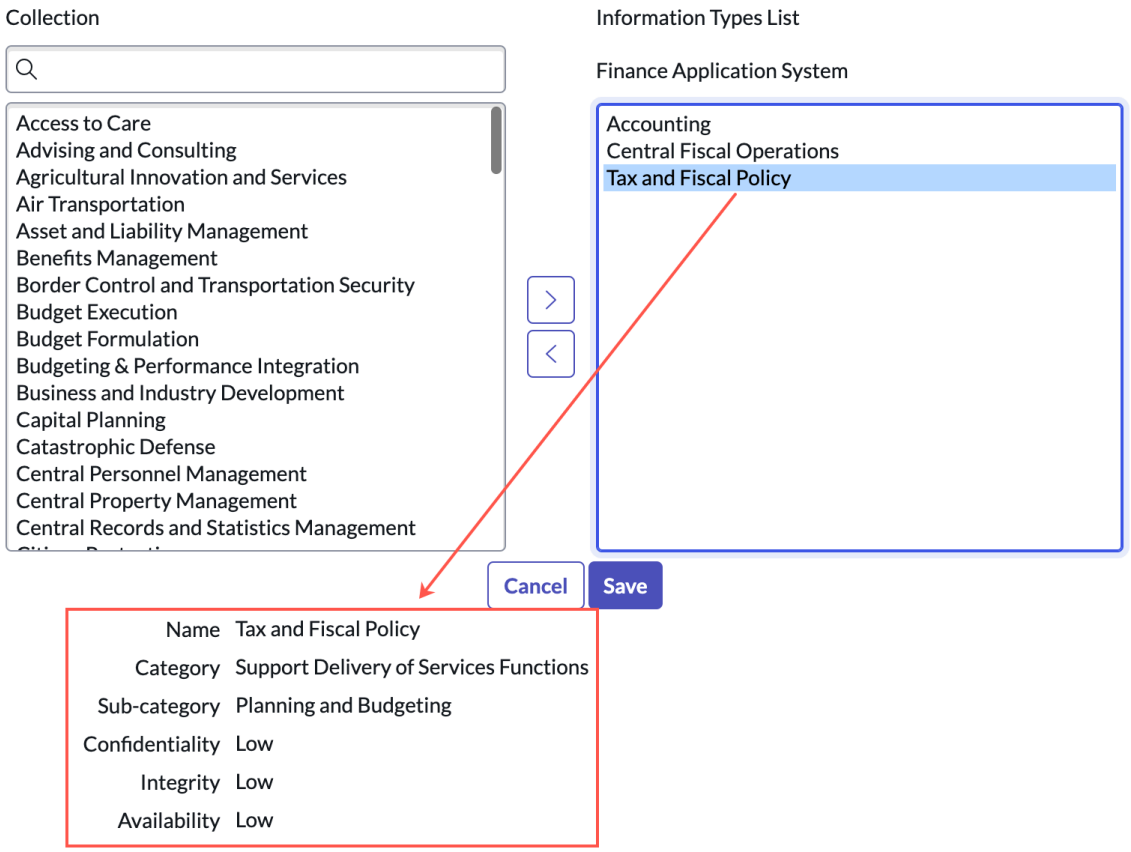
When you clicked **Categorize** on the Authorization Package form, an **Impact** field, an **Impact** tab, and an **Information Types** related list appeared on the form.

### Procedure

**1.** In the Information Types related list, click **Edit**.

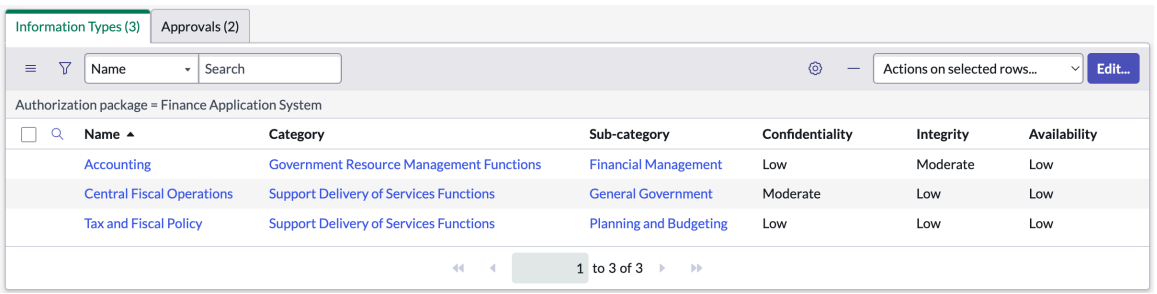
> **Note:** As you click on the information types, guidance about the selected information type appears, including name, categories, and the Confidentiality, Integrity, and Availability (CIA) ratings for the information type.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




2. Multi-select the information types you want to select for this authorization package and move them to the Information Type List box.
3. When you have completed your selections, click **Save**.

   The Information Types related list now contains the guidance information for the information types you selected.



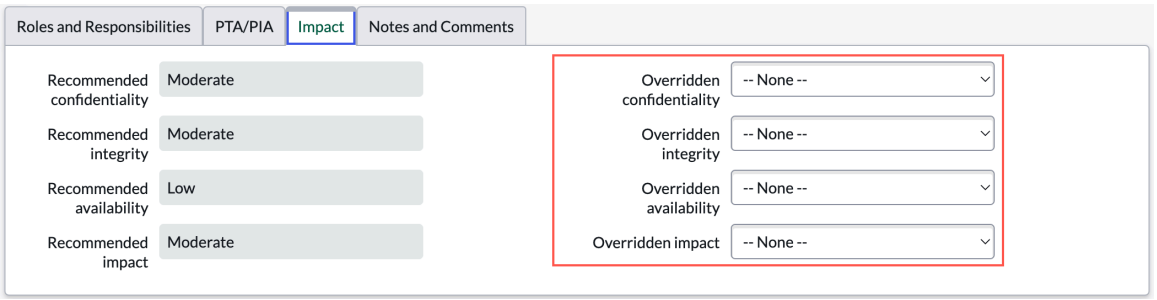

4. Click the **Impact** tab and review the recommended impacts for the information types you selected.

   **Note:** The impacts displayed in the **Recommended** fields reflect the worst-case scenario of the information types you selected. For example, if you selected an information type with High CIA levels, the **Recommended** fields under the **Impact** tab would all show **High** levels of risk. The CIA levels are used to calculate the overall impact of the information types you selected, which is now displayed in the **Impact** field.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. You can override any of the impact levels by modifying the **Overridden** fields on the right-hand side of the form and providing a justification.

   As you provide overrides, the **Impact** field is updated accordingly based on the update CIA levels.




**Important:** It is vital that the **Impact** field accurately reflects the impact of the data you are authorizing. All processes downstream from this point relies on that impact level. According to NIST guidelines, the number of controls you must implement depends on the Impact, as follows:

- High risk = 343 controls
- Moderate risk = 262 controls
- Low risk = 125 controls

6. After you have defined the impact, click **Request Approval**.
   An approval request is sent to the Authorizing Official, who will access My Approvals from the navigation pane and review the information in the package. When approval is received, the package transitions to the **Select** state.

## Select controls for an authorization package

When the impact levels for the package have been approved, it is time to select baseline controls in the Select step.

### Before you begin

Role required: To write to the sn_im_cont_baseline_control_objective table: sn_irm_cont_auth.system_owner, sn_irm_cont_auth.info_system_sec_officer, sn_irm_cont_auth.admin

To access the Mark as Not Applicable button: sn_irm_cont_auth.info_system_sec_officer, sn_irm_cont_auth.info_system_sec_manager, sn_irm_cont_auth.admin.

### About this task

When approval was received on the Authorization Package form, a **Control overlays** field and a series of **Controls** related lists appeared on the form.

### Procedure

1. Click the **Baseline Controls** related list.
   It shows the baseline controls for the calculated impact level of the package. The number of controls to be implemented (as defined by NIST) depends on the Impact level (High, Moderate, and Low).
2. You can perform the following actions on the list of controls.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Actions on Baseline Controls**

| Action | Description |
|---|---|
| Add controls to the list | Click **Add**, select the controls you want to add, and click **Create Baseline Controls**. |
| Add controls using a control overlay | Select a control overlay from the **Control overlays** field.<br><br>**Note:** Privacy overlays and other types of control overlays may be mandated by government agencies, but you can create them to add a given number of controls to your list. |
| Identify certain controls as being non-applicable | Select the controls, click **Mark as Not Applicable**, enter a justification, and click **Confirm**. The controls you marked this way are removed from the **Baseline Controls** list to the **Not Applicable Controls** related list. |
| Inherit controls from common controls | You can create common controls to which other, subordinate controls can be assigned so they can inherit risk guidance from them. For example, if you have a control that handles an entire facility, you can identify related controls that will inherit protection and compliance from the common control. To create a common control, select the control, click **Create Common Control**, click **OK** to confirm. For information on allowing a control to inherit from a common control, see Inherit protection and compliance from a common control. |

3. Click **Request Approval**.

   An approval request is sent to the Authorizing Official, who will access My Approvals from the navigation pane and review the information in the package. When approval is received, the package transitions to the **Implement** state.

   To send the package back to the Categorize state, click **Back to previous step**. All baseline controls will be removed and the package must get approval to advance again to the Select state.

## Set up baseline controls to generate controls and implement requirements

Use the baseline controls to inherit a control, mark a control as common, or create a hybrid control. Create a hybrid control to inherit requirements partially from common controls and the remaining requirements are created for the control that was generated from the baseline control.

### Before you begin

Role required: sn_irm_cont_auth.system_owner, sn_irm_cont_auth.info_system_sec_officer

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

Hybrid controls not only give you the ability to inherit partial requirements from common controls but also gives you the flexibility to make the best use of the common control requirements while self-implementing the remaining requirements for that control.

In CAM there are two ways to inherit controls from the control objectives sourced from NIST 800-53-r5:

Full inheritance

The control is inherited directly and completely. For example, if the common provider, Building A, provides a control objective that is fire prevention, and this control objective has about three different requirements, namely fire alarm, smoke detection, and sprinkling, then the control is directly inherited by identifying it as common control.

**Note:** A control associated with one authorization package can be a common provider to another authorization package if the control is marked as a Common control provider in its Authorization package, and that particular package must be in Monitor state. Only then it's called as a common control.

Hybrid inheritance

The control is partially inherited. Only one or a few of the control's requirements are inherited in this case. Considering the preceding example, hybrid inheritance is enabled in the following combinations:

- One of the requirement such as fire alarm can be inherited from Building A, and the other two requirements can be self-implemented.
- One of the requirements such as fire alarm can be inherited from Building A, and another requirement such as smoke detection can be inherited from Building B. The rest of which can be self-implemented.
- All requirements are inherited. This inheritance is not a partial inheritance because at least one of the requirements must be inherited and one must be self-implemented. Therefore this inheritance can't be termed as hybrid inheritance.

**Note:** The role and responsibility of the authorization package must be assigned to an Authorization official (AO) who must review and approve the authorization package when it moves from one state to another. The Information System Security Officers (ISSO) is required to mark a common control, create a hybrid control, or to identify a control as not applicable as these control objectives are sourced by NIST. After the Authorization official (AO) provides the approval, the authorization package moves to the Implement state.

### Procedure

1. Navigate to **All** > **Continuous Authorization & Monitoring** > **All Authorization Packages**.
2. Select an authorization package record that is in a **Select** state and has the Baseline controls added.
   In the **Select** state, all the baseline controls are added and you can identify the role of each baseline control. You can inherit a control, mark a control as common, or create a hybrid control.
3. To assign baseline controls from a common control provider as common controls:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select the control objectives in the Baseline Controls tab that you want to assign as common controls.

b. Select the **Mark as Common** button.

c. Select **OK** in the Confirmation pop-up.

d. Select the **Request approval** button to request approval.
After approval, the authorization package moves to Implement state. Before moving to the Implement state, the **Creates controls automatically** option in the control objective form must be true for all the baseline controls and hybrid controls. Otherwise, an error message pops up with the list of control objectives prompting you to make the **Creates controls automatically** option as true.

e. Select the control objectives link in the message and enable the **Creates controls automatically** option for all the control objectives in the respective control objective form.

After the authorization package is approved, the controls are created in the Controls tab. You can then move the authorization package to the Assess state. In this state, the Security Control Assessor (SCA) is required as an engagement lead, where the engagement is created to test the controls. After this state, the authorization package is moved to the Authorize state.

For an authorization package to be available as a common control provider for other authorization packages, it must be in the Monitor state. After the authorization package is moved to the Monitor state and the Common control provider flag is set as true for a few of the baseline controls, the controls that were generated for those baseline controls become common control providers for other authorization packages.

4. To inherit the requirements from a common control of a particular common control provider or create a hybrid control:

a. Select only one control objective in the Baseline Controls tab.

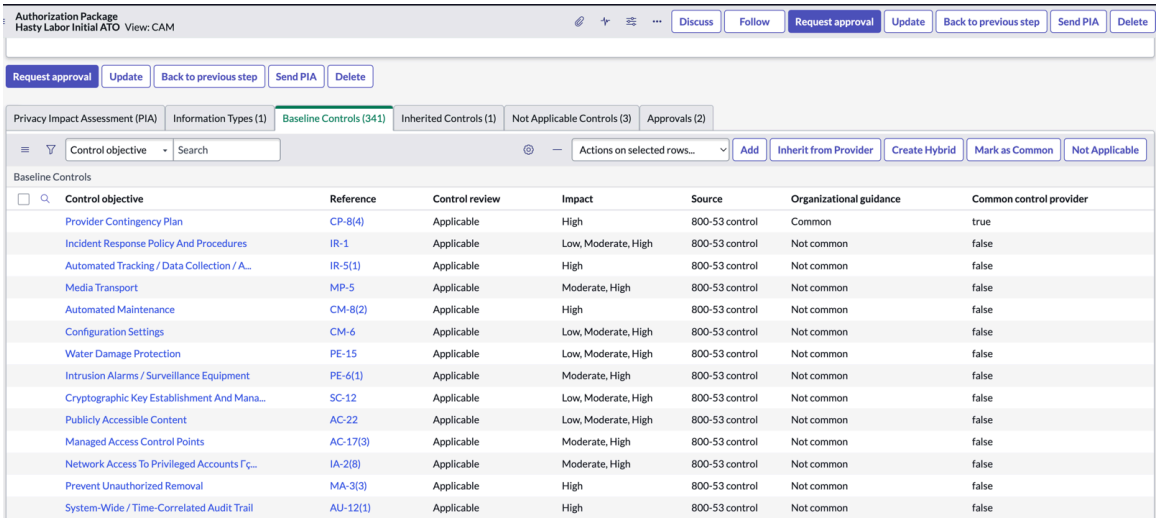
b. Select the **Create Hybrid** button.
The Create hybrid control pop-up lists the entities in groups. Grouping by entity helps when there are more requirement numbers added to the reference number of a control objective. You can inherit requirements partially from some of the common control providers, and self implement the rest of the requirements. If you select all control requirements from all the categories of providers for inheritance without a single self implemented requirement, then the requirements are not partially inherited but becomes full inheritance of all requirements, which is not allowed. At least one self-implemented requirement is required to create a hybrid control.

c. Select the requirements from the entity groupings, leaving one or more requirements for self implementation for that control.

d. Select the **Add** button.
The Hybrid Controls related list appears with the selected baseline controls. A baseline control is an m2m of a control objective and an authorization package.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### UI actions on baseline controls




**e.** Select the Display/hide hierarchical lists ( ▶ ) icon to see the inherited requirements. All the other requirements that are not listed here are self implemented.

> **Note:** Only common control providers with control requirements can be used to create hybrid controls.

**5.** To inherit controls from a common provider, select a control objective from the Baseline Controls related list, and click the **Inherit from Provider** button.

**a.** Select the Common control list in the Inherit from Common Control pop-up.

**b.** Select the controls that you want to inherit from.

**c.** Select the **Confirm** button.
The entities of the controls that you select become the common provider. For each of these authorization packages, there is an Inherited Controls related list. The **Inherited from** field in this related list gives you the information as to which control is the common control provider.

> **Note:** To inherit from a provider, which is a direct inheritance, there may not be any requirement for the control.

**6.** To mark a particular baseline control as not applicable so that it is out of the work flow and not allow controls to be generated:

**a.** Select a baseline control, and click the **Not Applicable** button.

**b.** Enter a note to justify your action in the **Justification** field.

**c.** Click the **Confirm** button.
This action changes the status of the selected baseline control to **Not implemented**.

In the **Select** state, you did the setup for the type of controls to be generated. After the setup is complete, you can approve the authorization package.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Select the **Request approval** button.
   The authorization package then moves to the **Implement** state. In this state, based on the setup, controls are created.

## Inherit protection and compliance from a common control

After you have created a common control, you can identify other controls that can inherit protection and compliance from that common control.

### Before you begin

Role required: sn_irm_cont_auth.system owner, sn_irm_cont_auth.info_system_sec_officer, or sn_irm_cont_auth.admin

### About this task

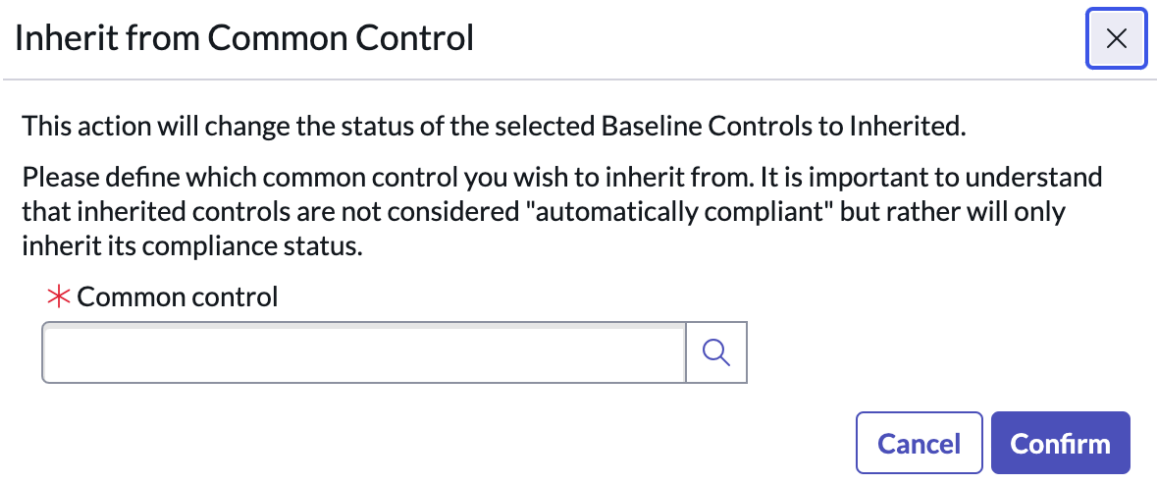
Consider this scenario. You and I are system owners. You own hundreds of servers and I own the facility in which they are installed. Based on the impact level of your authorization package, NIST recommends that you implement a given number of controls to protect your servers. However, you do not possess the means to implement two of them:

- Fire protection
- Visitor access control

You are aware that the facility has a fire suppression system, fire alarms, and smoke detectors. You also know that the facility has doors protected by a badge system. So you decide to inherit the protection in those controls from me, as well as the compliance. As long as I am compliant in terms of those controls, you are also compliant.

### Procedure

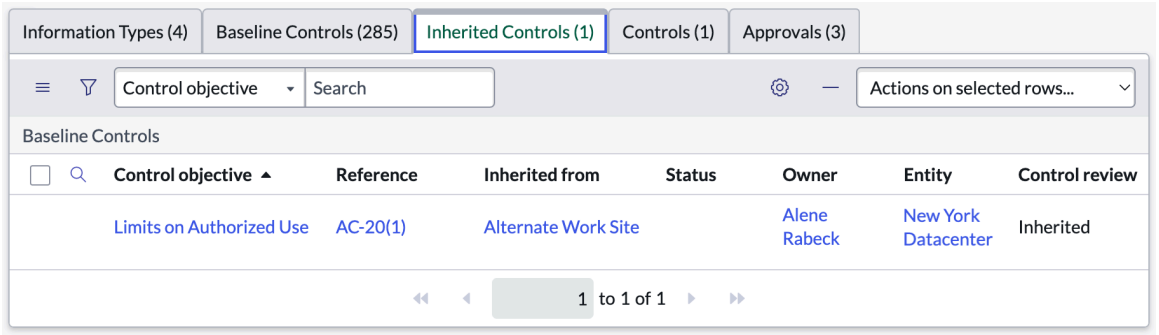
1. Navigate to **All** > **Continuous Authorization & Monitoring** > **All Authorization Packages**.
2. Open an authorization package in the Select state.
3. Select a control that you want to inherit protection and compliance from a common control.
4. Click **Inherit from Common Control**.




5. Select the common control you want to inherit protections from and click **Confirm**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Inherited Controls related list now shows the control objective and the common control from which it is inheriting protection and compliance.




## Implement controls

After you have selected controls for implementation, and performed any of the possible actions on them, you are ready for the Implement step.

### Before you begin

Role required: sn_irm_cont_auth.information_type, sn_irm_cont_auth.information_owner, or sn_irm_cont_auth.admin

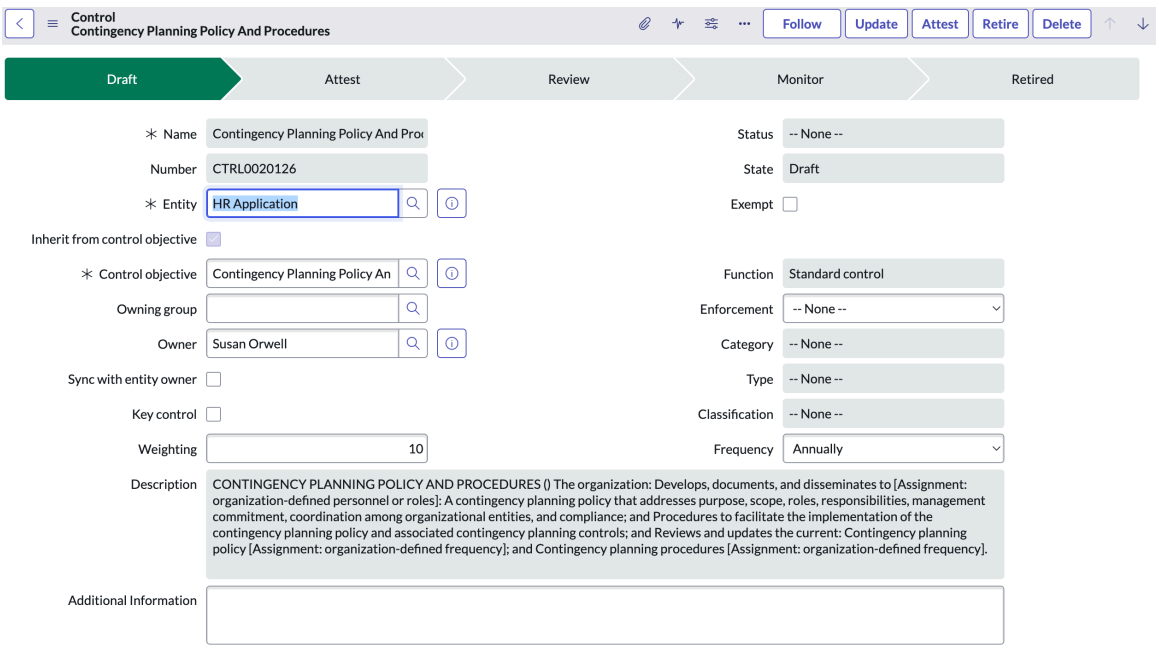
### About this task

When approval was received on the Authorization Package form, a **Percentage of controls implemented** field and a **Controls** related list appeared on the form.

The **Controls** related list contains all of the controls created from the control objectives within the selected authorization boundary.

### Procedure

1. From the list of controls, click the control number (with a CTRL prefix) to open the control.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. The implementation process performed by your system owner and other technical or security personnel employs the control management workflow inherent in the base GRC system.

   For details, see the following:

   - Manage controls
   - Manage control attestations
   - Manage control indicators

3. As you are implementing your controls, the **Percentage of controls implemented** field keeps track of your progress.
4. After you have completed the implementation process for all of your controls, click **Assess** to transition the package to the **Assess** state.

   To send the package back to the Select state, click **Back to previous step**. All active controls will be retired and the package must get approval to advance again to the Implement state.

## Assess, authorize, monitor, and generate reports

After you have completed the implementation process, you can assess internal and external controls, generate Plans of Action and Milestones (POA&M), and manage change requests and vulnerable items.

### Before you begin

Role required:

- sn_irm_cont_auth.system_owner
- sn_irm_cont_auth.info_system_sec_officer
- sn_irm_cont_auth.authorization_official
- sn_irm_cont_auth.info_system_sec_manager
- sn_irm_cont_auth.admin

### About this task

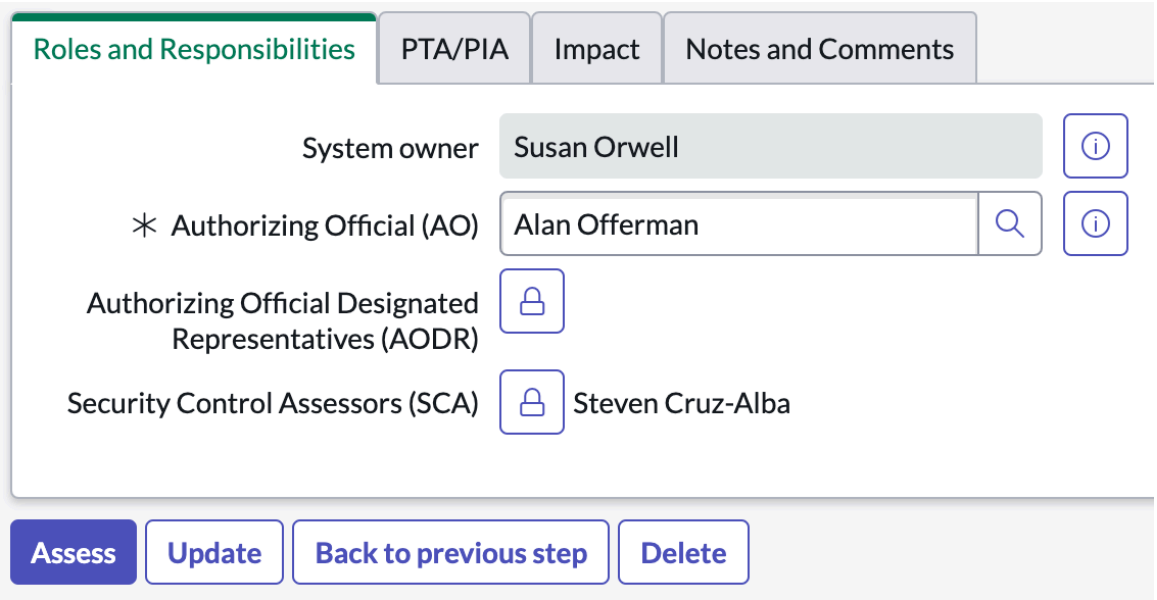
The Assess process is generally performed by a user other than the system owner or the personnel who implemented the controls.
The Assess state adds **Control Assessments** and **Risk Summary** related lists, as well as **POA&M**, **Change Requests**, **Security Incidents**, and **Vulnerable Items** tabs to the Authorization Package form.

**Note:** Performance issues have been observed in the Continuous Authorization & Monitoring application when a high volume of Change Request, Incident records, or both is related to a single Authorization Package. If you experience long transaction response times, consider performing the workarounds detailed in KB0861865.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

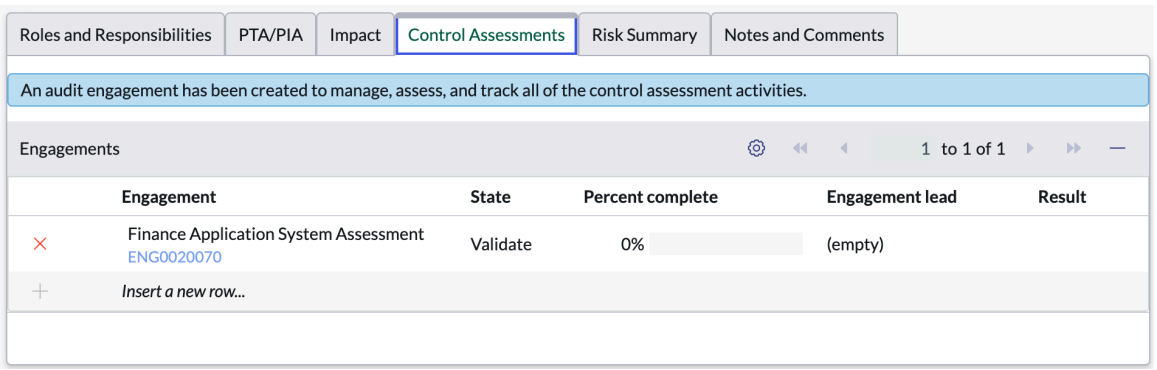
1. For an Authorization Package in the Implement state, select **Assess**.




**Note:** An Audit Engagement is automatically created.

To send the package back to the Implement state, select **Back to previous step**. The state of the engagement becomes Closed Incomplete. On selecting the **Assess** button, an engagement is created.

2. Select the **Control Assessments** related list to view the Audit engagement.

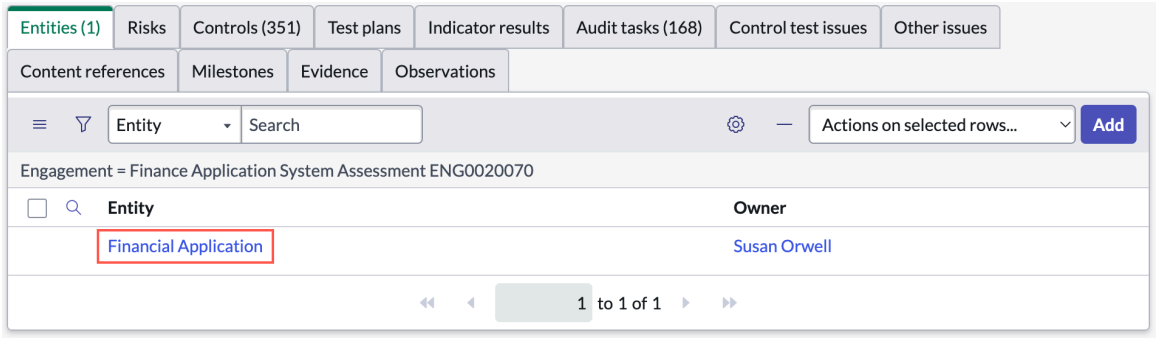



**Note:** The Audit Engagement is automatically assigned to the SCA.

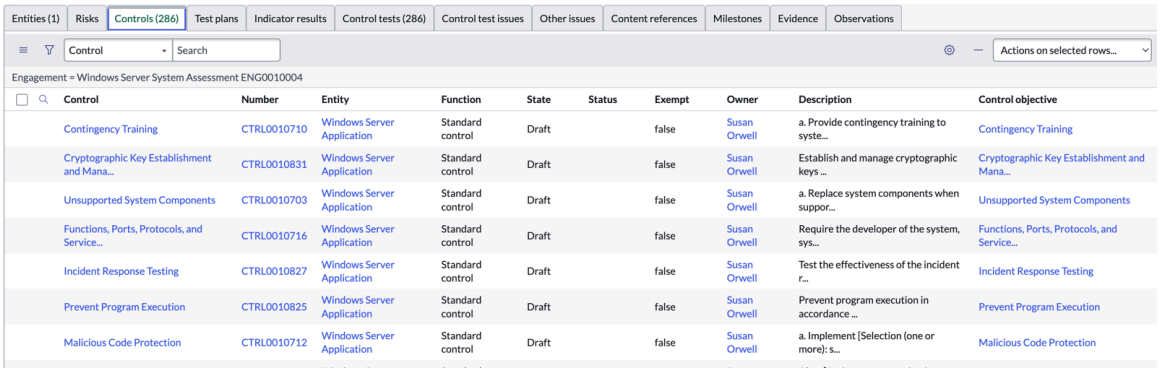
3. Select the engagement number to open it.

Notice that the **Entities** tab is displaying the authorization boundary for the package.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




4. Select the **Controls** tab to view all the controls that your team implemented.




5. Select the **Test plans** tab.
   Test plans are automatically created for the control. For more information on test plans, see Generate assessment procedure plans for a test plan.
6. Select the **Control tests** tab to view the tasks for assessing the controls.

> **Note:** **Audit tasks** tab in the Default view is renamed as **Control tests** tab in the CAM view. The names of the related list labels vary and are specific to the view that you select, which is either Default view or CAM view. You can change the view by selecting the Additional actions icon (☰), select CAM from the View list.
>
> For more information on test plans, see Determine control effectiveness of a control test.

7. In the Default view, select an audit task and perform the Design Test and Operation Test to judge the control's effectiveness.

   For details on this process, see Manage engagements.

> **Note:** Any issues that arise during the Assess phase appear in the **POA&M** tab. Additionally, any open Change Requests or Vulnerable Items targeting the system elements in the package appear under those tabs.

8. The system owner must review and document any POA&M issues, change requests, and vulnerable items that potentially threaten your systems.
9. When the review is complete, select **Authorize**.

> **Note:** In the Monitor state, continuous monitoring is achievable if you have indicators. If not, you can manually review the controls. For more information, see Manage control indicators.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can select the **Generate Report(s)** button to generate a FedRAMP System Security Plan (SSP) document for the authorization package in PDF format.

The package transitions to the **Authorize** state. When you're satisfied that all is in order, select **Request Approval**. An approval request is sent to the Authorizing Official, who will access **My Approvals** from the navigation pane and review the information in the package. When the approval is received, the package transitions to the **Monitor** state.

## Understanding assessment objectives in CAM

NIST 800-53A (National Institute of Standards and Technology) – assessment objectives are shipped by the ServiceNow base system with CAM application, which are mapped to the revision 5 control objectives.

**Note:**

- NIST SP 800-53 is the Security and Privacy Controls for Federal Information Systems and Organizations.
- NIST SP 800-53A is the Guide for Assessing the Security controls in Federal Information systems and organizations: Building Effective Security Assessment Plans.

Each of the test templates, which is imported by the ServiceNow base system to CAM users for control objectives sourced by NIST 800-53 revision 5, has assessment procedure templates. According to the NIST guideline, each assessment procedure template has an identifier and assessment objective. The assessment objective is the one that determines how the controls are tested.

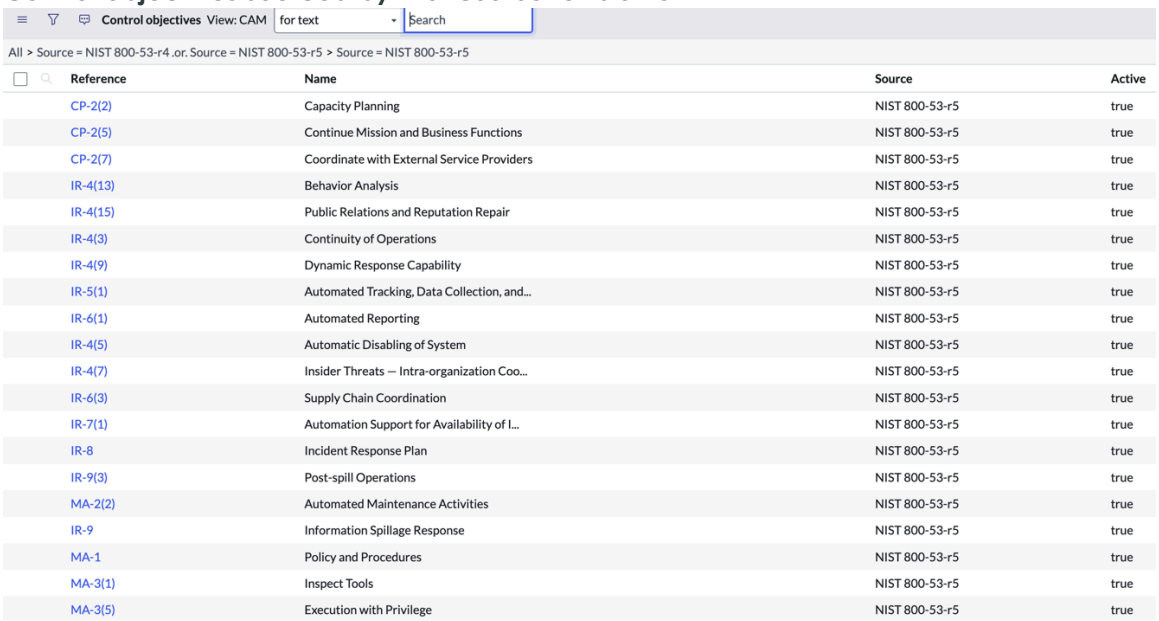
A new CAM view is available for the control test in which design effectiveness is removed and there is only operating effectiveness, which is named as Operational test.

In CAM, a control is tested at a more granular level with multiple assessment procedures. The control test measures the effectiveness of a control. The effectiveness of a control test is measured through its operating effectiveness and assessment procedure effectiveness, based on which the control effectiveness of the control test is determined. If the control test fails, it's indicative of the failure of the assessment objective as well.

Control test criteria such as Examine, Interview, and Test are available during control testing. These fields are read only, however you can update these descriptions at the test template and test plan levels. A set of assessment procedures is available as a related list while control testing. Assessment procedures are at the objective level, and can be marked as not applicable in addition to being effective, ineffective, and none.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Control objectives sourced by NIST 800-53 revision 5



Control objectives View: CAM | for text | Search

All > Source = NIST 800-53-r4 .or. Source = NIST 800-53-r5 > Source = NIST 800-53-r5

| Reference | Name | Source | Active |
|---|---|---|---|
| CP-2(2) | Capacity Planning | NIST 800-53-r5 | true |
| CP-2(5) | Continue Mission and Business Functions | NIST 800-53-r5 | true |
| CP-2(7) | Coordinate with External Service Providers | NIST 800-53-r5 | true |
| IR-4(13) | Behavior Analysis | NIST 800-53-r5 | true |
| IR-4(15) | Public Relations and Reputation Repair | NIST 800-53-r5 | true |
| IR-4(3) | Continuity of Operations | NIST 800-53-r5 | true |
| IR-4(9) | Dynamic Response Capability | NIST 800-53-r5 | true |
| IR-5(1) | Automated Tracking, Data Collection, and... | NIST 800-53-r5 | true |
| IR-6(1) | Automated Reporting | NIST 800-53-r5 | true |
| IR-4(5) | Automatic Disabling of System | NIST 800-53-r5 | true |
| IR-4(7) | Insider Threats — Intra-organization Coo... | NIST 800-53-r5 | true |
| IR-6(3) | Supply Chain Coordination | NIST 800-53-r5 | true |
| IR-7(1) | Automation Support for Availability of I... | NIST 800-53-r5 | true |
| IR-8 | Incident Response Plan | NIST 800-53-r5 | true |
| IR-9(3) | Post-spill Operations | NIST 800-53-r5 | true |
| MA-2(2) | Automated Maintenance Activities | NIST 800-53-r5 | true |
| IR-9 | Information Spillage Response | NIST 800-53-r5 | true |
| MA-1 | Policy and Procedures | NIST 800-53-r5 | true |
| MA-3(1) | Inspect Tools | NIST 800-53-r5 | true |
| MA-3(5) | Execution with Privilege | NIST 800-53-r5 | true |

## Generate assessment procedure plans for a test plan

Use the test plan that is automatically generated for a control, which is in an assess state, to view and determine if the control is assessed in accordance with the assessment procedure plan.

### Before you begin

Role required: sn_irm_cont_auth.system_owner, sn_irm_cont_auth.info_system_sec_officer, sn_irm_cont_auth.authorization_official, sn_irm_cont_auth.info_system_sec_manager, sn_irm_cont_auth.admin

### About this task

Assessment procedure plans are generated for the test plan of a control based on the control objective. Each control objective has a particular test template, and assessment procedure templates are created for this test template. Test plans are generated from the test template of a control objective. And, the assessment procedure plans are generated from the assessment procedure template.

### Procedure

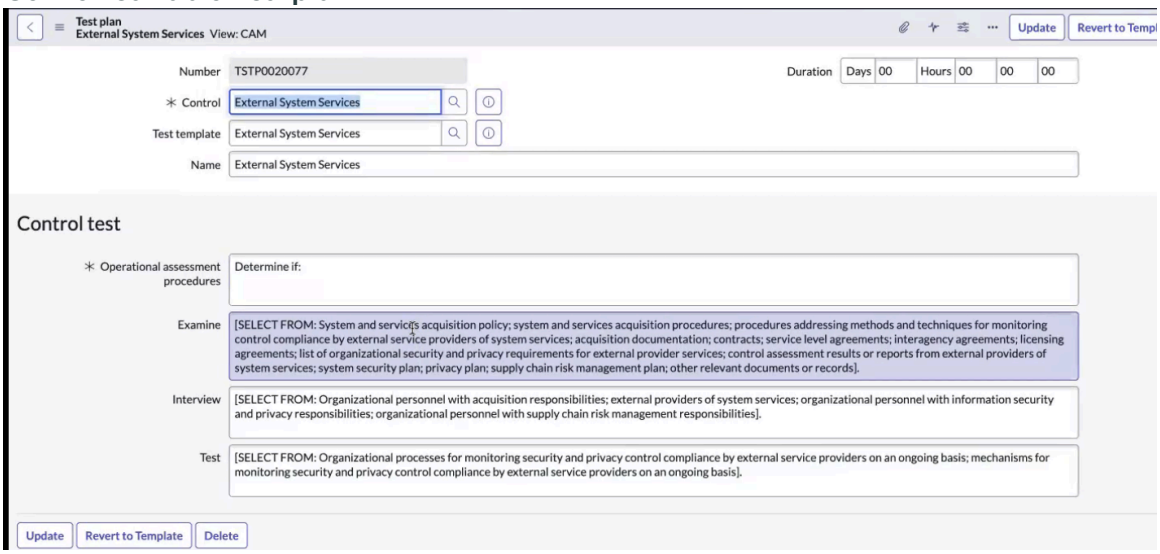
1. Navigate to **All** > **Continuous Authorization & Monitoring** > **All Controls**.
2. Select the control that has been assessed for which the test plans are created.
3. Select the Test plans related list and click the test plan link in the **Number** column.
   In the Test plan form that opens, you can view the test plan details such as the name of the test template from which this test plan is generated, and the name of the control that is to be assessed based on this test plan.

   Test templates are shipped by the base system for NIST 800-53 revision 5 controls. Test plans are automatically created from these test templates. Whenever the authorization package moves from the Implement state to the Assess state, the control tests are created from these test plans that are generated from the test templates.

   In the Control test section, there are four field descriptions such as **Operational assessment procedures**, **Examine**, **Interview**, and **Test**. Examine, Interview, and Test descriptions are drawn from the NIST guideline and added to the Test template form. You can update the field descriptions as required here in the Test plan form.

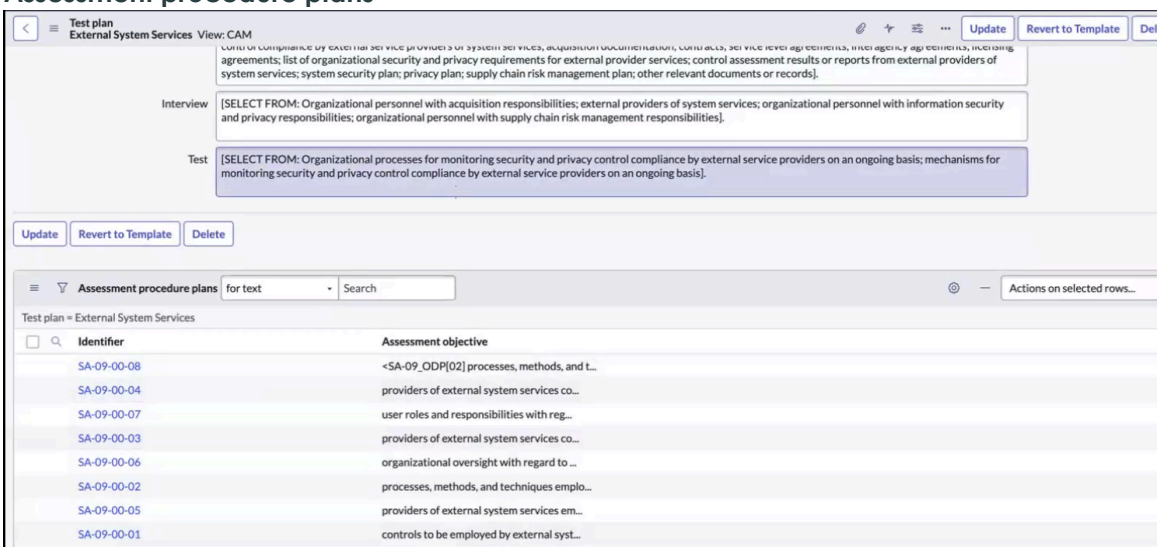
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Control test tab of test plan




4. To update the descriptions, select the field and update the text.
5. Select **Update** after editing the descriptions.
6. To revert to the original control test descriptions in the associated test template, select the **Revert to Template** button.
7. Select **OK** in the Confirmation pop-up to confirm your decision.
8. To open the Assessment procedure plan and view the assessment objective, select the link in the **Identifier** column of the Assessment procedure plans section.
   In the Assessment procedure plan form, you can view the identifier of the assessment procedure plan, the name of the test plan, and the assessment objective. Assessment objective is the guideline as to how to assess the control. If necessary, update the objective.

### Assessment procedure plans




9. To view the control tests that are generated to assess the control, navigate to the Controls tests related list of the Engagement form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Determine control effectiveness of a control test

Apply the objective effectiveness of the assessment procedures and the operating effectiveness of the control test to determine the control effectiveness of the control test. An assessment procedure is applied to check the control test at a granular level.

### Before you begin

Role required: sn_irm_cont_auth.system_owner, sn_irm_cont_auth.info_system_sec_officer, sn_irm_cont_auth.authorization_official, sn_irm_cont_auth.info_system_sec_manager, sn_irm_cont_auth.admin

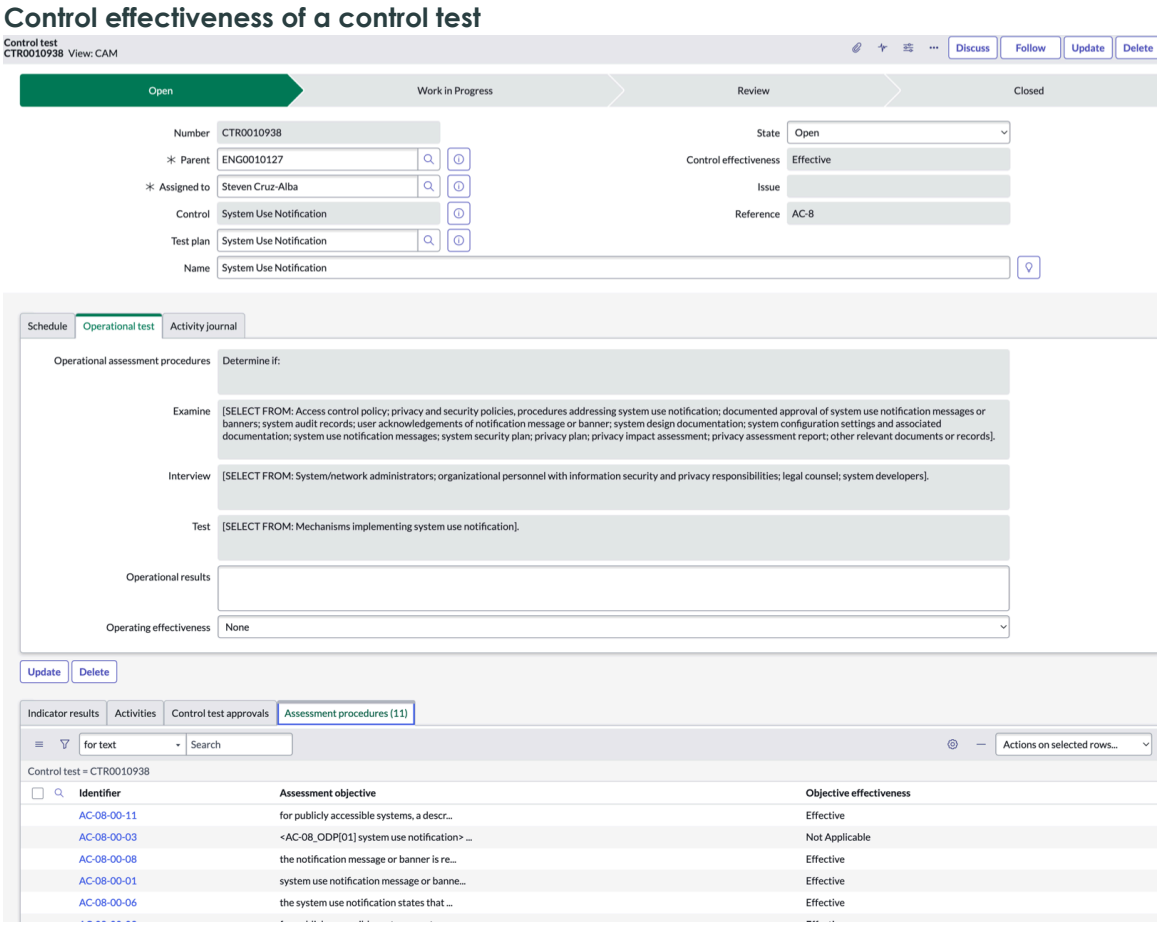
### Procedure

1. Navigate to **All** > **Continuous Authorization & Monitoring** > **All Engagements**.
2. Select the engagement.
3. Select the **Control tests** tab and click a control test link in the **Number** column.
4. In the Control test form that opens, you can view the effectiveness of the control in the **Control effectiveness** field.
5. Select the **Operational test** tab to view the operating effectiveness of the control test.

   **Note:** The **Examine**, **Interview**, and **Test** fields are pre-populated from the NIST control objectives, and aren't editable at the control test level. If you must edit any of these descriptions, you can do so in the test plan form. See Generate assessment procedure plans for a test plan.

6. Select the Assessment procedures related list to view the objective effectiveness of all the assessment procedures.
   The number of assessment procedures generated is exactly equal to the number of assessment procedure plans that were generated from the test plan.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The values of the operating effectiveness of a control test are:

- None
- Ineffective
- Effective

The values of the objective effectiveness of an assessment objective are:

- None: Indicates that the assessment procedure hasn't been analyzed or assessed yet.
- Effective
- Ineffective
- Not Applicable: Indicates that the assessment procedure isn't valid or not required for this control test check.

The Control effectiveness of the control test is determined by:

| Operating effectiveness | Objective effectiveness | Control effectiveness |
|---|---|---|
| Effective/Ineffective/None | Any one is Ineffective | Ineffective |
| Effective | Not applicable/None/ Effective | Effective |
| Ineffective | Not applicable/None/ Effective/Ineffective | Ineffective |
| Ineffective | Ineffective | Ineffective |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Operating effectiveness | Objective effectiveness | Control effectiveness |
|---|---|---|
| None/Effective | Effective | Effective |
| None | One is Effective and another Ineffective | Ineffective |
| None | One is None and another is Not applicable | None |

As long as the control test is in the Open or Work in Progress state, it does not matter if the objective effectiveness of the Assessment procedures is None. However, you cannot move the control test to the Review state until you mark every assessment objective as either Effective, Ineffective, or Not Applicable. An error message pops up to indicate that you must check the assessment objective and move it out of the None state, so as to move the control test to the Review or Closed Complete state.

7. Select the link in the Identifier column of the Assessment procedures related list to view the Assessment procedure form.
   All fields in the form are read only except the **Objective effectiveness** field, which you can edit if the control test is either in Open or Work in Progress state. The **Objective effectiveness** field is read only in the Review state, or in any closed states such as Closed Complete, Closed Incomplete, and Closed Skipped.
8. If you update the objective effectiveness value of the assessment procedure, select **Update** to save your changes.

## Defining a control's requirements at the level of control objective

You can break down a control at a more granular level as requirements when you generate the control at the control objective level.

Defining control requirements helps:

- Security Control Assessor (SCA): To assess each requirement of the control individually if there are different aspects to the control testing.
- Authorization official (AO), Information System Security Officer (ISSO) and Information System Security Manager (ISSM): To understand the requirement that failed, which lead to the non-compliance of the control, instead of evaluating the failure of the control as a whole.
- Attestation respondent identified for a control: To respond at the control requirements level, which is at a more granular level, rather than at the control level.

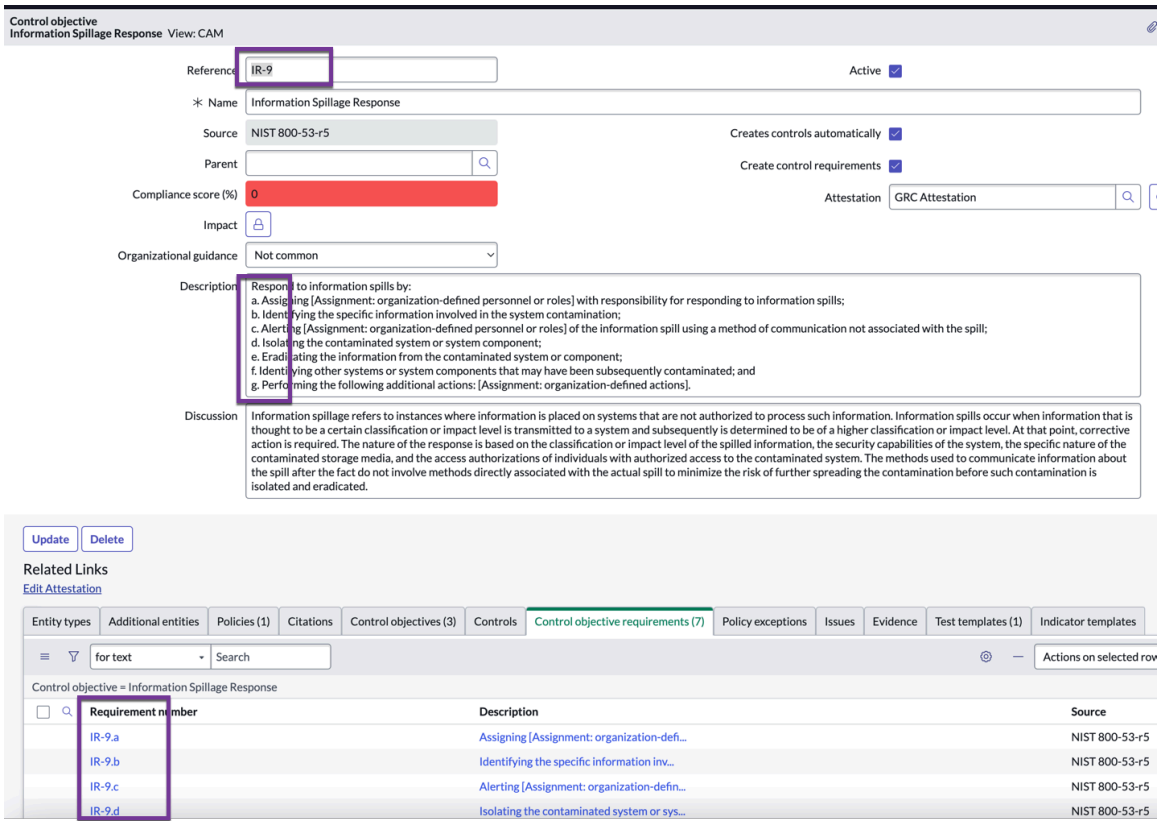
As a CAM user you can break down the controls to control requirements, manage the requirements more efficiently, attest them individually, and have the package authorized. You can also define the requirements and create them at the control objective level when controls are generated.

## Creating NIST content from control objective description as control requirements

The ServiceNow base system ships the control requirements generated from the NIST 800-53 revision 5 control objectives to CAM users. The **Description** field of the Control objective form lists the requirements broken down as sub-points with sub-numbers. The Reference of the control objective is clubbed with each sub-number or the clause in the **Description** field and referenced as a **Requirement number** in the Control objective requirement. For example, if the Control objective reference is IR-9, and the description of the control objective starts with a sub-number (a.), then the two are clubbed together to generate the first control objective

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

requirement as IR-9.a, with further sub-numbers added to it if available. Therefore, if there are about seven sub-descriptions, then seven control requirements are generated.




### Control requirement details in the CAM view of Control objective and Control forms

The CAM view of the Control form has fields that have been added to capture the control requirement details.

To accommodate the control requirement details in the CAM view of a Control objective form and Control form, a Control objective requirements related list and Control requirements related list are added, respectively.

**Note:** The views of the Control objective form and Control form in the CAM view are almost the same as the Control objective and Control forms used in Policy and Compliance Management. However, some fields have been removed and some added in the forms to capture the control requirement details.

## CAM view of a Control objective form

### CAM view of the Control objective form

| Field | Description |
|---|---|
| Reference | Unique numerical identifier or the content reference number. |
| Name | Name of the control objective. |
| Source | Source of the control objective, which is NIST 800-53 revision 5 for which the test templates are provided. |
| Parent | Control objective that is not a child of the current control objective. This relationship is to avoid cyclic parent – child relationship. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### CAM view of the Control objective form (continued)

| Field | Description |
|---|---|
| Compliance Score (%) | Compliance score percentage calculated for this control objective and its color code:<br>• 80 and higher in green<br>• 80 to 50 in yellow<br>• below 50 in red |
| Active | Option to activate a control objective. |
| Creates controls automatically | Option to indicate that controls are automatically created when an entity is associated from the Additional entities related list by selecting the **Add relationship** button and the entity. |
| Create control requirements | Option to generate control requirements automatically for the control objective.<br>**Note:** If there are no control objective requirements, then there won't be any control requirements either. |
| Attestation | Reference to the metric type. **GRC Attestation** is chosen by default.<br>**Note:** If the user changes the control attestation, the related control objective attestation type is changed also. |
| Impact | Potential impact to business functions because of loss of confidentiality, integrity, or availability of target and data. |
| Organizational guidance | Security control definitions from NIST, which when designated as common control definitions by organizations, are inheritable by one or more organizational targets. |
| Description | Description of the control objective. |
| Supplemental guidance | If it is control objective sourced by NIST 800-53 revision 4, then a direction for the control objective implementation. |
| Discussion | If it's a control objective sourced by NIST 800-53 revision 5, then content-related information that is sourced by NIST. |

Control objectives are just guidelines and aren't specific to an entity or any object. You can link one control objective with any control objective requirement, and one control objective requirement with any number of control objectives, as the relationship between the control objective and the control objective requirement is many-to-many.

### Control objective requirements related list

| Field | Description |
|---|---|
| Requirement number | Requirement number of the control objective. |
| Active | Option to make the requirement active. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Control objective requirements related list (continued)**

| Field | Description |
|---|---|
| Description | Detailed description about the requirement for the control objective. |

In the Control objective requirements related list, you can select the **New** button to create a requirement for the control objective if necessary, based on which requirements are generated. Or, select the **Edit** button to add an existing control objective requirement to the control objective.

**Note:**

- If the control objective is in the Inactive state, you cannot create or add control objective requirements. Therefore, the **New** and **Edit** buttons are not available.
- If the control objective requirement is inactive, you cannot add a control objective to the control objective requirement.

## CAM view of the Control form

**CAM view of Control form**

| Field | Description |
|---|---|
| Reference | Unique identifier. |
| Name | Name of the control. |
| Number | Unique identification number of the control. |
| Entity | Related entity.<br>**Note:** If you change the state of the entity to Active from Retired state, then the manually created control on the entity also moves to the Draft state. |
| Control objective | Related control objective. |
| Owner | User who owns the policy.<br>**Note:** The owner is always added as a respondent. The control owner that you select belongs to the owning group. |
| Status | Control status. Possible choices are:<br>• **Compliant**<br>• **Non-compliant**<br>• **Not applicable** |
| State | Control state. Possible choices are:<br>• **Draft**: When the control is created from a control objective, controls are in this state. In this state, all compliance users can modify the control. Only available when creating a one-off control. One-off controls are possible but not recommended. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**CAM view of Control form (continued)**

| Field | Description |
|---|---|
| | • **Attest**: When you select the **Attest** button and take attestations, the control moves to this state.<br><br>**Note:** When a control is set back to draft, the attestation is canceled.<br><br>• **Review**: Controls are automatically moved to review from the attestation phase.<br>• **Monitor**: In this state, all compliance managers can move the control from review to monitor.<br>• **Retired**: Compliance managers or administrators can move a control from Monitor to Retired.<br><br>**Note:** When a control is retired:<br>◦ Associated indicators don't run<br>◦ Associated attestations are canceled<br>◦ Changes to associated control objectives don't update the control |
| Authorization package | The authorization package that the control is associated with or originating from. |
| Frequency | List of options:<br><br>• Event Driven<br>• Daily<br>• Weekly<br>• Monthly<br>• Quarterly<br>• Semi-Annually<br>• Annually<br><br>Attestation is sent based on the value selected for the control or control requirement.<br><br>**Note:** For information on the difference between the **Frequency** field for a control and the **Attestation Frequency** field in an entity, see KB0694607. |
| Weighting | Value used to calculate the control score effectiveness. Based on the control weighting, in the control score effectiveness value is calculated. |
| Owning group | Group that owns the policy. |
| Control allocation | Type of control that is created. It can be either system specific or hybrid. |
| Description | Description of the control. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### CAM view of Control form (continued)

| Field | Description |
|---|---|
| Discussion | Content-related information from NIST 800-53 revision 5. |
| Supplemental guidance | If it's a control sourced by NIST 800-53 revision 4, then a direction for the control implementation. |
| Implementation statement | An explanation on how the control is going to be implemented.<br><br>This is a required information if the control is created from an authorization package and in the Draft state. |
| Attestation | |
| Take attestation at requirement level | Option to send attestations at the control requirement level and not at the control level. |
| Attestation | Select from a list of options.<br><br>• Other attestation types can be configured.<br>• If this field is populated, then the **Attestation Respondents** field automatically becomes mandatory, and the owner is made the respondent.<br><br>**Note:** If the user changes the attestation type in the control objective, all the related controls are changed also. |
| Attestation respondents | • Users assigned to the attestation of this control.<br>• Only a user with the sn_grc.user role can be added as a respondent.<br><br>**Note:** When both the **Attestation** and **Attestation respondents** fields are set, attestations are created when you select **Attest**. |
| Activity Journal | |
| Additional comments | Public information about the control. |
| Activities | Message logs of control state change. |

### Control requirements related list

| Field | Description |
|---|---|
| Number | Control requirement's unique number. |
| Requirement number | Reference number. |
| Control | Control to which the control requirement is associated. |
| Status | Status of the control requirement. |
| State | Requirement state. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Control requirements related list (continued)**

| Field | Description |
|---|---|
| Frequency | Control frequency. |
| Description | Description of the control requirement. |
| Attestation | |
| Attestation | Attestation metric type. |
| Attestation respondents | User who attests the control requirement. |
| Activity Journal | |
| Additional comments | Information about the control requirement.<br><br>When the control objective requirement is dissociated, that is removed or deleted, the control requirement becomes manual. This information is logged in this field. |
| Activities | Message logs of control requirement's state change. |

## Modify control requirement's implementation status at the control level

Approve the authorization package when it is in Select step to create controls. After approval, the authorization package moves to the Implement step and the controls are generated. You can still modify the control requirement implementation status at the control level.

### Before you begin

Role required: sn_irm_cont_auth.system_owner

### About this task

Controls are generated for all the baseline controls that have the value as **Applicable** or **Hybrid** in the **Control review** field of the Baseline control tab. Additionally, the type of control that is generated is determined by the **Control allocation** field in the Control form, which can be either **System specific** or **Hybrid**.

- Controls are created for all controls coming directly from baseline controls that are system specific and marked as Applicable.
- Controls are created for hybrid controls, which will have requirements based on the hybrid setup.
- Controls are not created for inherited controls.

All the controls are generated in the **Implement** state, however you can still update the setup at the control level in this state.

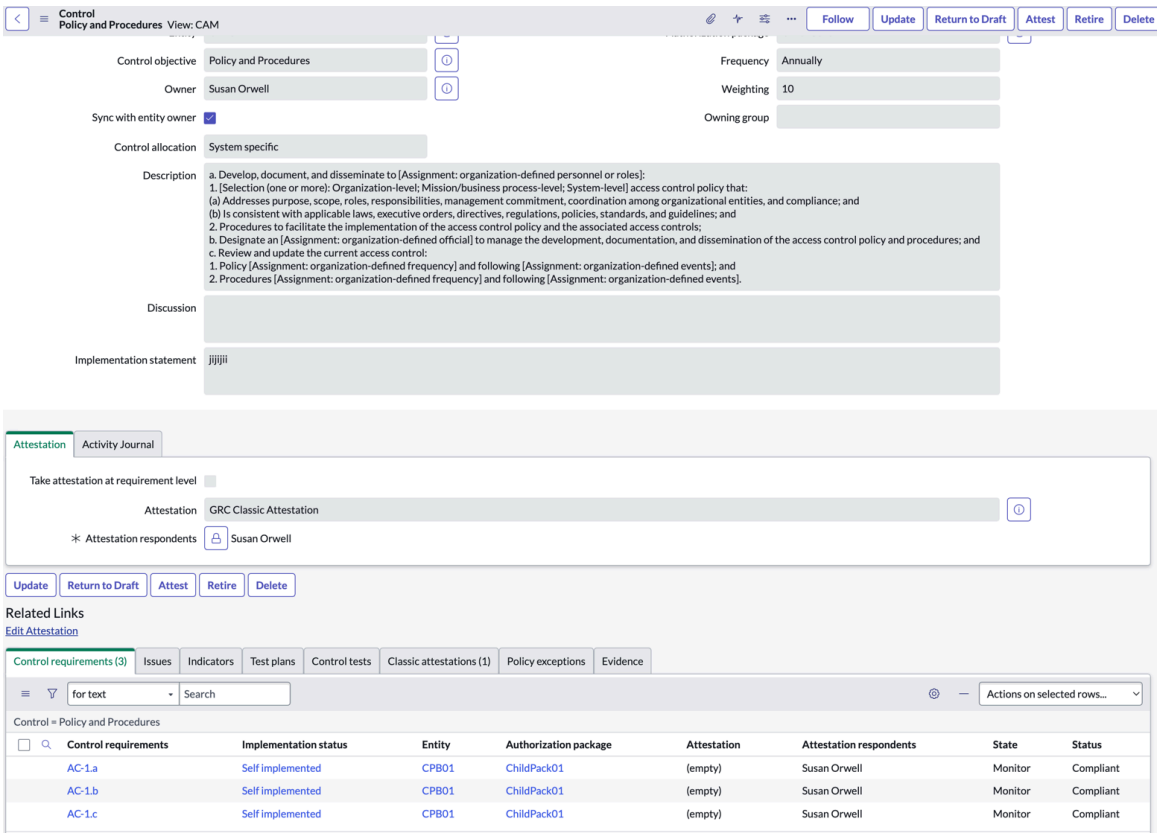
### Procedure

1. Navigate to **All** > **Continuous Authorization & Monitoring** > **All Authorization Packages**.
2. Select the authorization package that is in the Implement state, for which you want to modify the control setup.
3. Select the Controls related list.
   The number of controls generated is displayed in the Controls related list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
Number of Controls = Baseline Controls + Hybrid Controls
```

4. Select the control to modify its setup.




5. To change the provider for a particular requirement, select the control requirement in the Control requirements related list.

   a. Select the **Change Provider** button.

   b. Select the **Common control** list field in the Inherit from Common Control pop-up. The filter query lists only those providers that you have not already selected for you to choose from.

   c. Select the **Confirm** button.

   On selecting confirm, the query filter removes the current provider from the authorization package of the Control requirements list. You can also select the Activity Journal related list to see the message that the provider has been changed, logged in the **Activities** field.

   You can only change the provider for the requirement using the **Change Provider** button. However, this action does not make the requirement automatically compliant by changing the provider.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Important:** You must not make a selection that changes the value in the **Control allocation** field of the Control form when you do this setup change. If it is a hybrid control and if this requirement is the only one that has the **Implementation status** as **Self implemented**, and by changing the provider to another control that has the control allocation value as **System specific** where the **Implementation status** of all its requirements are **Inherited**, then the control allocation is no longer hybrid as all its requirements are inherited.

For a hybrid control at least one requirement should be inherited and at least one should be Self implemented.

- All the requirements are Self implemented for a system specific control.
- At least one requirement must be Self implemented and the rest can be inherited for a hybrid control. If it is inherited, then the control requirements are inherited from a provider, which comes from the Baseline Controls related list.

6. To change the implementation status of the control requirements to self implemented, select those control requirements in the Control requirements related list.
   a. Select the **Convert to Self implemented** button.
   b. Select **Yes** in the Confirmation pop-up.
   Your control requirement selections can also include those requirements that are already in self implemented status. However, after this operation, only those requirements that were in Inherited status are converted to Self implemented.

   By this UI action, the existing m2m relationship between the control provider and the control is deleted. Thereafter, a new m2m relationship is created with the new selection. A message describing the change is also logged in the **Activities** field of the Activity Journal tab of the Control form.

7. To convert a control requirement from self implemented to inherited status, select the requirement in the Control requirements related list.
   a. Select the **Convert to Inherited** button.
   b. Select the **Common control** list field in the Inherit from Common Control pop-up.
   You can select from all the providers that are available to inherit that control requirement. After this UI action, the previous self implemented control requirement is deleted, and the new requirement that you selected is inherited from the provider. Simultaneously, the set up is also changed at the authorization package level in the Hybrid Controls related list, where the requirement selections of that baseline control reflects your change.

   If this is the only requirement that is in self implemented status for the hybrid control, then you cannot convert it to inherited.

8. To see the list of control requirements for a hybrid control, select the Display/hide hierarchical lists ( ) icon that gives you a hierarchy view.
   You can use in the Hybrid Controls related list as well. Additionally, you can do the above three actions – Convert to Self implemented, Convert to Inherited, and Change Provider – from the Controls related list also.

   From the Implement state you can move back to the Select state. When you do so, all the controls that were active and created in the Implement state will be deleted or retired.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When you are in Select state, you can modify the setup for all the hybrid controls and generate controls once again.

9. To revert a hybrid control as a baseline control, select the control in the Hybrid Controls related list.

   a. Select the **Return to Baseline Control** button.

   b. Select **OK** in the Confirmation pop-up.
   This action deletes the previous Requirement selections for the hybrid control. It also updates the baseline control's **Control review** field from **Hybrid** to **Applicable**. You can set up the steps for this baseline control and select the **Create Hybrid** button. You can view the current control requirements available for this control. Four setup changes are possible for a hybrid control to return to being a baseline control:

   - It must be a system specific control while moving back to Select state, and you can mark this as inherited.
   - Convert from hybrid to inherited.
   - Move the control back to baseline, mark it as common, and make it a common provider.
   - Convert the control to not applicable so that it is out of the work flow and controls will not be generated for this.

   You can also revert an inherited control as a baseline control by selecting the **Return to Baseline Control** button in the Inherited Controls related list. In this case, the baseline control's **Control review** field is updated from **Inherited** to **Applicable**.

## Impact of associated compliance objects on control requirements

Control objective requirements are created for a control objective. The control requirements are generated for all the controls that are associated with a control objective. However, a control or a control requirement can become non-compliant because of an attestation failure or issue creation at either of the two levels.

## Associating an issue to a control requirement and its impact on control status

An issue can be created for a control requirement through an attestation. You can enable the **Take attestation at requirement level** option to send out the attestations for all the control requirements instead of sending an attestation for the control at the control level. The **Take attestation at requirement level** option is in the Attestation related list of the Control form.

If the attestation fails, then an issue is created. The issue created because of an attestation failure has the **Issue source** field tagged as **Requirement Attestation Failure**.

You can view the control requirement reference in the **Control/Risk** field of the Details related list in the Issue form.

You can close the issue by providing a response and saving it in the Issue form. Your response can be either **Remediate** or **Accept**.

- If you select Remediate and set the state of the issue to Closed Complete, then the control requirement becomes compliant, provided there is no other open issue on the control requirement.
- If you select Accept, then you imply that the issue still exists and that you accept it. In this case, even if you close the issue with no other open issues, the status of the control requirement is still non-compliant.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Therefore, to make the control requirement status compliant you must set your response to Remediate and not Accept.

Whenever the control requirement becomes non-compliant, the control also becomes non-compliant. When the status of the control requirement becomes compliant, there are two more criteria to be checked at the control level:

- There should be no open issue on the control.
- Not even one control requirement of the control must be non-compliant.

If these two conditions are satisfied, then the status of the control becomes compliant. Otherwise, the status of the control remains non-compliant despite the control requirements status being compliant.

- If the control and control requirements are in Draft or Attest state, then you can pass the attestation to make the control and control requirement compliant.
- If the control and control requirements are in the Review or Monitor state, you can move the state **Back to attest** and pass the attestation to make the control and control requirements compliant.
- If the control requirement is in Monitor or Retired state, then you cannot create an issue for the control requirement.

## Impact of indicator test and control test on the control requirement status

A control requirement can become non-compliant because of an issue that is created as a result of an attestation failure on this control requirement. If there is no open issue on the control or even if you close the issue that existed, the control requirement remains non-compliant. Although the indicator task **Result** is **Passed**, the control remains non-compliant because one of the control requirements of the control is non-compliant. You must explicitly make the control requirement of the control as compliant, and then when the indicator test is passed, then the control becomes compliant.

The same is the case for a control test also.

## Changes in control state and its impact on control requirements

Draft

All control requirements are generated when the control is in Draft state.

When the control moves to Draft state, the associated control requirements also move to Draft state.

Attest

When the control moves to Attest state from any other state, then all the control requirements of the control also move to Attest state irrespective of the **Take attestation at requirement level** option.

**Note:** When you select the **Attest** button, you have the option to take a single attestation at the control level or take multiple attestations at the control requirements level, which is guided by the **Take attestation at requirement level** option.

Review

For control-level attestation, when the **Take attestation at requirement level** option is not selected, after attestation is complete the control moves to Review

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

state. Simultaneously all associated control requirements of the control move to Review state.

For control requirement level attestation, when the **Take attestation at requirement level** option is selected, then the attestation is sent to all the Attestation respondents of all the control requirements individually. When the attestation is completed, irrespective of the attestation outcome at the control requirement level as Pass or Fail, the control requirement moves to Review state. If the attestation passes, the status of the control requirement becomes compliant, and if it fails, the control requirement becomes non-compliant. After the attestation is completed for all the control requirements and when they are all in the Review state, then the control moves to the Review state.

Monitor

When the control moves to Monitor state, the associated control requirements also move to Monitor state.

Control requirements remain in the Monitor state as long as the control remains Active and hasn't moved back to Draft or Attest state.

Retired

When the control is Retired, the control requirements move to Retired state.

Deleting a control removes or deletes all the control requirements associated with the control.

For more information on attestation flow scenarios, see the Attestation workflow for Control and Control requirements [KB0555561] article in the Now Support Knowledge Base.

## Impact of inherited requirements on the life cycle of a control

1. If one of the control requirements becomes non-compliant, then the corresponding control is also non-compliant.
2. If one of the inherited control requirements becomes non-compliant, then the control is also non-compliant.
3. If an attestation for a control fails, an issue is created, and the control becomes non-compliant.
4. If an attestation for a control requirement fails, an issue is created, and the control requirement becomes non-compliant. So, the associated control also becomes non-compliant.
5. If one of the inherited control requirements of a hybrid control retires in such a condition, an automated issue is created. The reason for issue creation is reflected in the **Issue source** field of the Issue form as **Provider Control Retired**. An appropriate message is also logged in the Activity related list of the Issue form. To resolve the issue, you can either change the common control provider or convert the control requirement to self implemented.
6. If the control is in Draft state and one of its requirements is retired, then you cannot move the control from Draft to Attest state.

**Note:** For more information, see the Operational changes and their impact on the process flow of control and its requirements [KB1587264] article in the Now Support Knowledge Base.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Control requirement generation and upgrade steps

The **Creates controls automatically** and **Create control requirements** options in the control objective form and the state of the authorization package are important to create control requirements.

## Control requirement generation logic

If you enable the **Creates controls automatically** and **Create control requirements** options in the control objective form, then the item generation flow is triggered automatically to create controls and control requirements, respectively. Depending on the state of the control, the generated control requirements' state changes.

If the **Create control requirements** option is selected when the authorization package moves from the **Select** to the **Implement** state, the controls are generated. At the same time, control requirements for the control objective requirements are also generated. Control requirements would be generated only if the control objective requirements are present and if the flag is true. If the control objective requirements are present but the flag is false, then the control requirements would not be generated.

If while creating the control objective, the flag was set as false and the requirements weren't generated, you can still generate the control requirements by selecting the flag and saving the control objective record, provided the controls associated with this particular control objective have control objective requirements, and the controls are Active and in the Draft state. If the controls are in any state other than Draft, then control requirements would not be generated. However, if, for example, the control was in the Monitor state and is moved back to Draft state, then control requirements would be generated provided the **Create control requirements** option is selected.

New control objective requirements added

The same is the case when you add control objective requirements to a control objective using the **New** or **Edit** button in the Control objective requirements related list.

Update

If you update the description of a control objective requirement, then the description of the corresponding control requirement is updated provided the control is in the Draft state. If the control is in any other state, then the description is updated when the control moves back to Draft state.

Delete

If a few of the control objective requirements of a control objective are removed, then correspondingly the control requirements of the control cannot be removed, instead they are marked as a Manual requirement. This condition is true for controls in any state. Later, if the control moves to Draft state, then you can remove the manual tag from these requirements. On the other hand, if a new control is created after some of the control objective requirements are removed, then the new control does not have the requirements that were removed but only the existing number.

If the authorization package moves from the Implement to Select state, then all the associated controls of CAM are retired, and correspondingly all the requirements associated with them are also retired. All these actions are handled by item generation.

## Mandatory upgrade steps

The following upgrade setup actions take place on upgrading to Utah release:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. The **Authorization package** field and **Control allocation** field in the Control form are newly added. The values in these fields are populated for the existing CAM controls.
2. For all NIST 800-53-revision 5 control objectives, the **Create control requirements** option is set to **True** by default in the Control objective form.
3. The control requirements are created for all the existing controls, from NIST 800-53-revision 5 control objectives, which are in the Draft state.

## Continuous Authorization and Monitoring overview reports

You can view Continuous Authorization and Monitoring reports and other visualizations on the Overview.

The reports you can view depend on your user role, as follows:

- To view reports available to users with the CAM Administrator [sn_irm_cont_auth.admin] role, navigate to **Continuous Authorization and Monitoring** > **CAM Overview**.
- To view reports available to users with the Authorization Official [sn_irm_cont_auth.authorization_official] role, navigate to **Continuous Authorization and Monitoring** > **AO Overview**.
- To view reports available to users with the Security Control Assessor [sn_irm_cont_auth.sec_control_assessor] role, navigate to **Continuous Authorization and Monitoring** > **SCA Overview**.

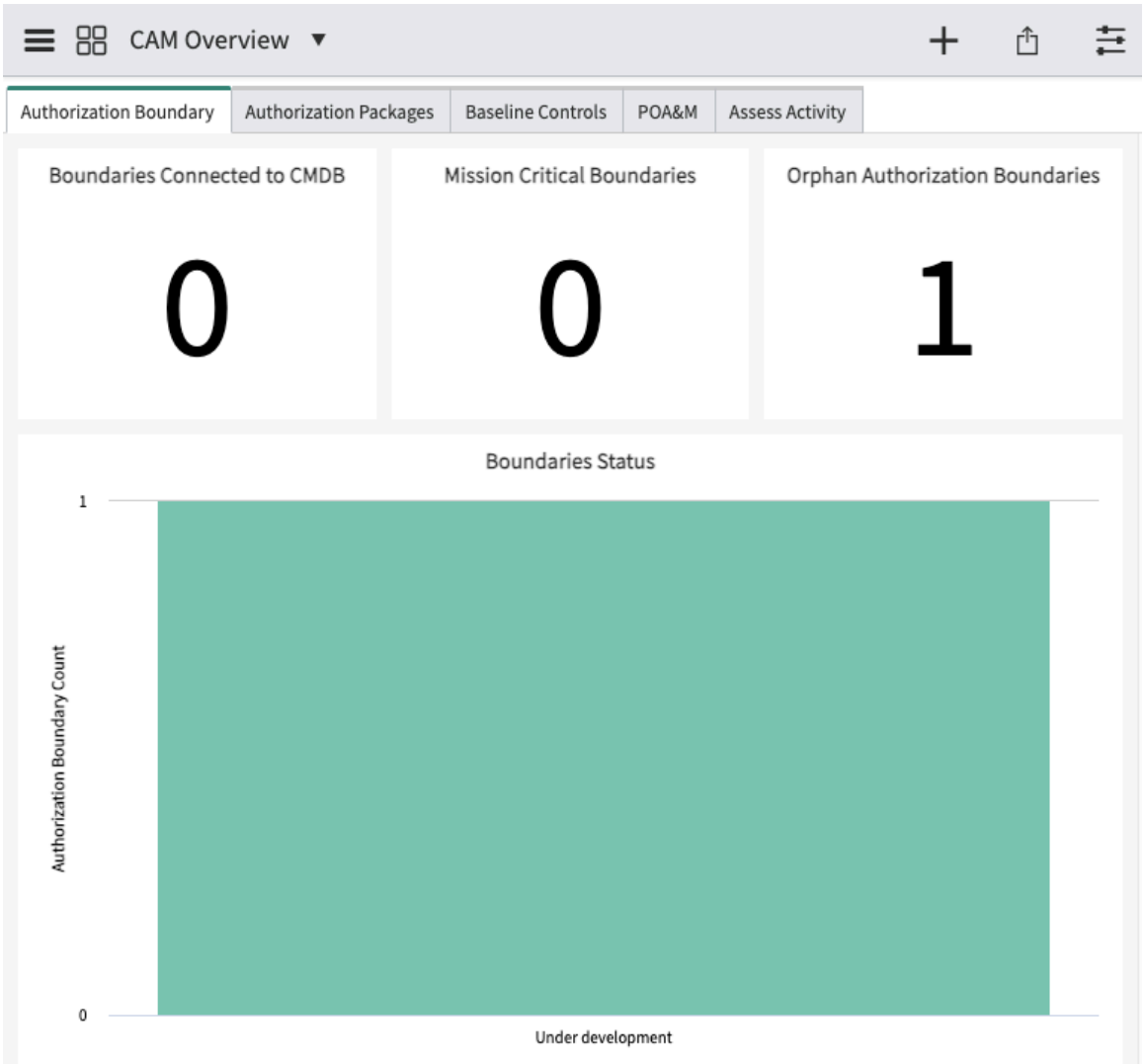
### Reports available from the CAM Overview module

Users with the CAM Administrator [sn_irm_cont_auth.admin] role can view the reports in the CAM Overview module.

The CAM Overview module includes reports on five tabs.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**CAM Overview tabs**




## CAM Overview - Authorization Boundary tab

The reports on the Authorization Boundaries tab provide a general overview of the authorization boundaries defined in your system.

**Reports on the Authorization Boundary tab**

| Report | Description |
|---|---|
| Boundaries Connected to CMDB | The number of authorization boundaries defined to work with your CMDB. |
| Mission Critical Boundaries | The number of authorization boundaries defined as being mission critical. For more information, see Define authorization boundaries. |
| Orphan Authorization Boundaries | The number of authorization boundaries not related to an authorization package. |
| Boundaries Status | The number of authorization boundaries in each state. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## CAM Overview - Authorization Packages tab

The reports on the Authorization Packages tab provide a general overview of the authorization packages defined in your system.

### Reports on the Authorization Packages tab

| Report | Description |
|---|---|
| Packages with Overridden Impact | The number of authorization packages with an impact that has been overridden. For more information, see Categorize the authorization package. |
| Packages Pending Approval | The number of authorization packages for which approval has been requested, but that have not yet received approval. |
| Packages by Impact | The number of authorization packages categorized by impact levels. |
| Packages by Step | The number of authorization packages categorized by steps (for example, Monitor, Access, Select, and so forth). |

## CAM Overview - Baseline Controls tab

The reports on the Baseline Controls tab allows you to easily track the state of all authorization packages across the agency.

### Reports on the Baseline Controls tab

| Report | Description |
|---|---|
| Packages with Inherited Controls | The number of authorization packages that contain baseline controls inherited from a common control. |
| Packages with Common Controls | The number of authorization packages for which common controls were created and implemented. |
| Packages with Unimplemented Controls | The number of authorization packages for which common controls were created, but have not yet been implemented. |

## CAM Overview - POA&M tab

The reports on the POA&M tab provide visibility into how your systems are providing, inheriting, and implementing controls.

### Reports on the POA&M tab

| Report | Description |
|---|---|
| Pending POA&Ms | The number of Plans of Action and Milestones (POA&M) that are pending authorization. |
| POA&Ms with Milestones | The number of POA&Ms that contain milestones. |
| POA&Ms with Acceptance Tasks | The number of POA&Ms that contain acceptance tasks. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Reports on the POA&M tab (continued)**

| Report | Description |
|---|---|
| Overdue POA&Ms | The number of POA&Ms that have overdue milestones or acceptance tasks. |
| POA&Ms by State | The number of POA&Ms categorized by state. |
| Packages with POA&Ms | The number of authorization packages that contain POA&Ms. |
| POA&Ms by Priority | The number of POA&Ms categorized by priority. |
| POA&Ms by Response | The number of POA&Ms categorized by responses. |

## CAM Overview - Assess Activity tab

The reports on the Assess Activity tab allows you to gain increased visibility and reduce management effort around a;; POA&Ms in your agency. For more information on these reports, see Create an engagement with advanced planning.

**Reports on the Assess Activity tab**

| Report | Description |
|---|---|
| Inadequate Engagements | The number of engagements closed with an inadequate result. |
| Satisfactory Engagements | The number of engagements closed with a satisfactory result. |
| Adequate Engagements | The number of engagements closed with an adequate result. |
| Controls by Engagement | The number of controls categorized by engagements. |
| Audit Task Breakdown | Audit tasks grouped and/or stacked by task type, assigned user, top task, or state. |
| POA&M Breakdown | POA&Ms grouped and/or stacked by engagement, state, or response. |
| Control Test Results | The number of completed control tests, broken down by overall control effectiveness rating. |
| Engagement Results | An overall count of audit engagements conducted for each entity. The chart is stacked to display the overall audit results for each entity. |
| Overdue Audit Tasks | List of open audit tasks that have exceeded the planned end date. |

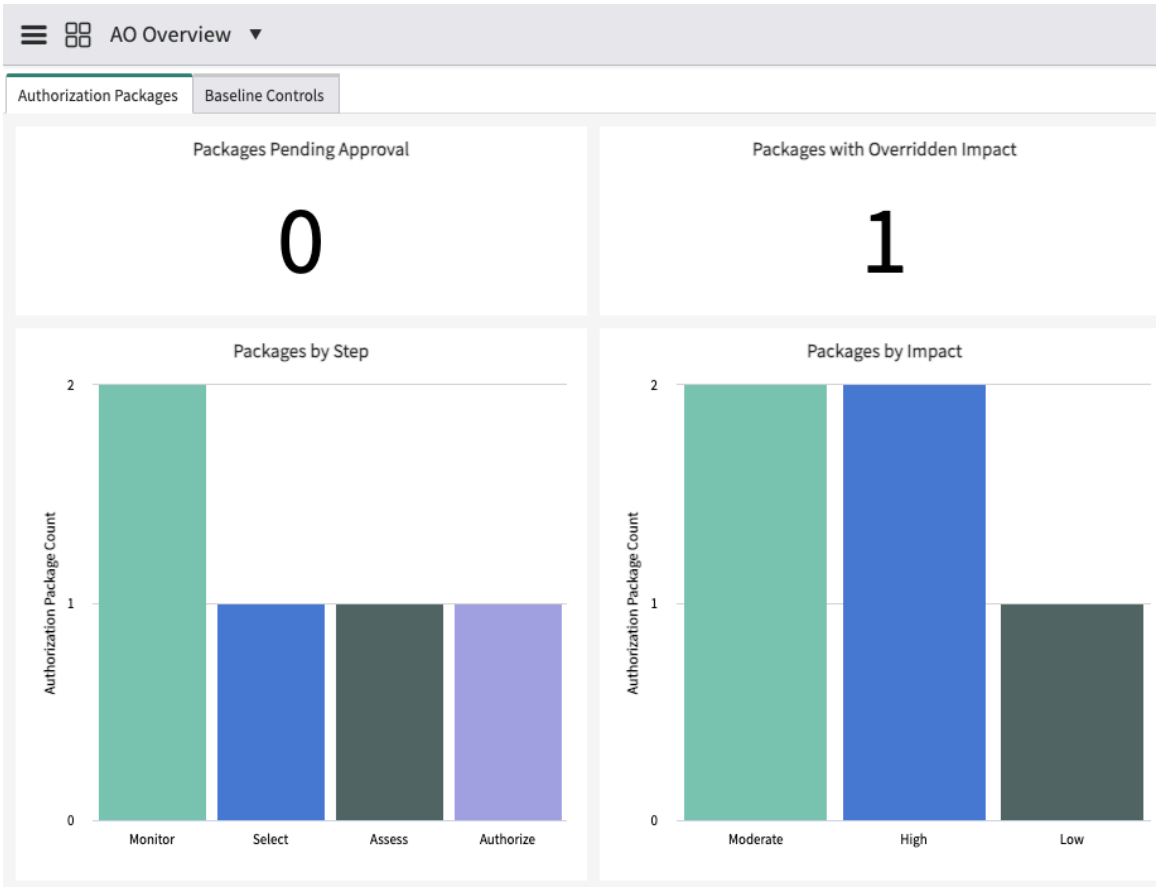
## Reports available from the AO Overview module

Users with the Authorization Official [sn_irm_cont_auth.authorization_official] role can view the reports in the AO Overview module.

The AO Overview module includes reports on two tabs.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### AO Overview tabs




## AO Overview - Authorization Packages tab

The reports on the Authorization Packages tab reduce effort and time with central visibility into the state of all packages.

### Reports on the Authorization Packages tab

| Report | Description |
|---|---|
| Packages Pending Approval | The number of authorization packages for which approval has been requested, but that have not yet received approval. |
| Packages with Overridden Impact | The number of authorization packages with an impact that has been overridden. For more information, see Categorize the authorization package. |
| Packages by Step | The number of authorization packages categorized by steps (for example, Monitor, Access, Select, and so forth). |
| Packages by Impact | The number of authorization packages categorized by impact levels. |
| Pending Approvals | A list of all packages pending approval. |

## AO Overview - Baseline Controls tab

The reports on the Baseline Controls tab provide a general overview of the baseline controls in your system.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Reports on the Baseline Controls tab**

| Report | Description |
|---|---|
| Packages with Unimplemented Controls | The number of authorization packages for which common controls were created, but have not yet been implemented. |
| Packages with Inherited Controls | The number of authorization packages that contain baseline controls inherited from a common control. |
| Packages with Common Controls | The number of authorization packages for which common controls were created and implemented. |
| Compliance Score Percentage | Compliance score percentages for policies grouped by name or number. |

## Reports available from the SCA Overview module

Users with the Security Control Assessor [sn_irm_cont_auth.sec_control_assessor] role, can view the SCA Overview module.

The SCA Overview module includes the following reports.

## SCA Overview

The reports under SCA Overview allow you to view and manage control assessments as they occur to reduce effort and decision-making time.

**Reports on the SCA Overview**

| Report | Description |
|---|---|
| Adequate Engagements | The number of engagements closed with an adequate result. |
| Satisfactory Engagements | The number of engagements closed with a satisfactory result. |
| Inadequate Engagements | The number of engagements closed with an inadequate result. |
| Controls by Engagement | The number of controls categorized by engagements. |
| Audit Task Breakdown | Audit tasks grouped and/or stacked by task type, assigned user, top task, or state. |
| POA&M Breakdown | POA&Ms grouped and/or stacked by engagement, state, or response. |
| Control Test Results | The number of completed control tests, broken down by overall control effectiveness rating. |
| Engagement Results | An overall count of audit engagements conducted for each entity. The chart is stacked to display the overall audit results for each entity. |
| Overdue Audit Tasks | List of open audit tasks that have exceeded the planned end date. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Operational Resilience

Operational Resilience is the ability of an organization to respond to the adverse operational events by anticipating, preventing, recovering from, and adapting to such events.

## Operational Resilience overview

In today's changing business landscape, an organization may face various operational risks at unanticipated times. Every function of your business plays an important role in maintaining and promoting operational resilience. For example, the Risk team must have the right governance in place to identify and respond to operational risks. The IT team must identify and address the existing and potential threats.

The ServiceNow® Operational Resilience application empowers your organization to continue to provide your business services in the face of adverse operational events, such as pandemic, extreme weather, or hacking. With Operational Resilience, you can monitor and report data from multiple places and recover from the potential disruptions quickly, with a minimal impact on your customers.

## Get started

| | | |
|---|---|---|
| **Explore**<br>  <br>Learn about Operational Resilience | **Configure**<br>  <br>Configure the Operational Resilience application | **Use**<br>  <br>Set up Operational Resilience classic Workspace |
| **Manage**<br>  <br>Manage Operational Resilience tasks | **Reference**<br>  <br>Components installed with Operational Resilience | |

## Learn

What is operational resilience?

## Additional resources

- Ask or answer questions in the GRC community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Developer training
- Developer documentation

## Exploring Operational Resilience

The Operational Resilience application provides a complete view of your operational resilience status including the service details, entities, and the posture of the core areas of your business.

### Operational Resilience overview

The Operational Resilience application helps your organization to achieve a uniform vision and build resilience across different business functions. By using the Operational Resilience application on one platform, various teams can monitor the health of their services in one place as shown in the following example.

**Uniform vision with Operational Resilience**




The Operational Resilience application helps different departments to build their operational resilience effectively:

- IT departments can automate their processes and track the availability and functioning of the failover systems of their applications.
- HR departments can have clear visibility on the market trends, resource pools, and retention risks.
- Facilities departments can focus on implementing the major improvements that help you to manage your day-to-day business operations with low maintenance.
- Security departments can address the physical vulnerabilities and cyberthreats efficiently.
- Finance teams can manage the contractual issues, supply chain risks, and overall finances effectively.
- Risk teams can analyze their potential risks and mitigate their service impact on the business operations.

### Business Continuity Management and Operational Resilience

Business Continuity Management implements an approach wherein it builds a plan to respond quickly to a disruption that may impact your entire organization. Operational

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Resilience defines the steps that an organization must proactively take to prevent any operational disruptions.

Business Continuity Management is about analyzing the business disruptions, preparing a disaster recovery plan, and responding to a crisis event at the business process level. Operational Resilience implements a holistic approach about providing a complete end-to-end service delivery. Operational Resilience is about proactively monitoring the resilience statistics and ensuring that the service delivery happens at any cost.

As stated earlier, Business Continuity Management operates at the business process level. On the other hand, Operational Resilience provides a clear understanding of your company's operational resilience statistics on the dashboard. It includes the statistics for Business Continuity Management, Vulnerability Response, and so on.

## Operational Resilience workflow

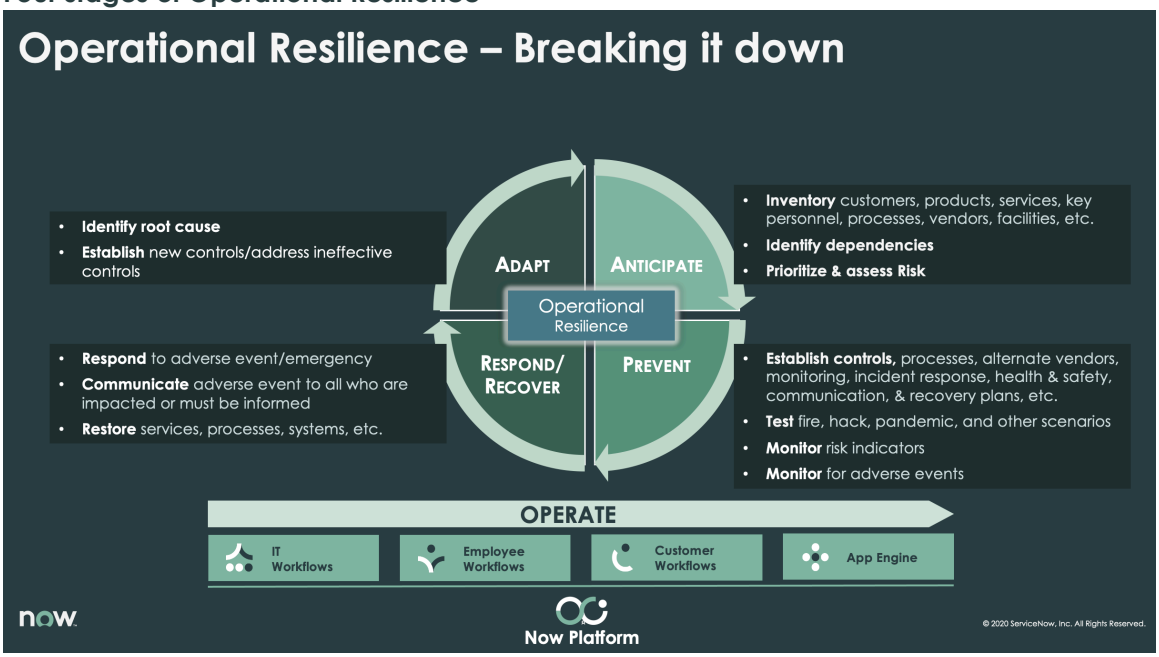
The Operational Resilience application provides a continuous four-stage workflow that helps your resilience managers and administrators to achieve your organization's safety and well-being. You can prepare for and cope with the adverse events by anticipating, preventing, recovering from, and adapting to such events. The stages of operational resilience are shown in the following example.

**Operational Resilience workflow**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Four stages of Operational Resilience




To build resilience for your organization, analyze each stage in the resilience life cycle:

1. Anticipate: When disastrous events happen, it is not always obvious which services, people, and processes are critical. Organizational silos, poor data, and different tools can impede your understanding of risks and cross-business dependencies. A lack of prioritization and planning can mean imprecise decision making.

   To overcome these challenges, the Operational Resilience application helps you to perform a what-if scenario analysis to better plan for best, worst, and expected outcomes. The application helps you to prepare for what you must protect and identify the areas to prioritize, according to your business and risk context.

2. Prevent: Most operational procedures are designed for efficiency rather than for risk and compliance. Businesses often over-rely on the manual corrective controls, rather than the automated preventative controls. Early warning of risks or adverse events can be thwarted by manual processes and fragmented data. Such practices can cripple your response to disastrous events.

   The Operational Resilience application can guide you through establishing sufficient controls that reduce the likelihood of potential problems in time to mitigate them effectively. With risk and compliance activities incorporated into your daily work, operations run smoothly with fewer efforts. Intelligent processes and policies help you unlock new efficiencies. Continuous monitoring triggers an immediate and targeted incident response.

3. Respond/Recover: Many businesses are organized in such a way that they are unable to respond to adverse events quickly or safely. Communication internally, or with vendors and suppliers is poor. Split-second decisions can worsen the situation, especially when information is incomplete or outdated.

   Continuity plans that are created using the Operational Resilience application can help you prevent an out-of-control escalation of an incident. A pre-approved and tested recovery plan prepares you to respond to the situations effectively, reduces the risks, and improves the recovery time.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Adapt: Operational resilience means you can quickly and easily bounce back from disasters. However, when these events occur, they are not often seen as learning opportunities. But they are. If you look at them in that way, you have a chance to improve your protective measures and respond effectively to the next event. Learning from these events and adapting can lead to minimized impacts and speedier recovery.

   Adverse events, such as fire, extreme weather, pandemics, or data breaches, offer lessons about what could work better. The Operational Resilience application, can help you collect data, assess results, and feed conclusions back to your teams. Visibility to the past provides business leaders with a vision of better operational performance in the future.

### Operational Resilience benefits

The Business Continuity Management application provides the following benefits:

| Benefits | Features | Users |
|---|---|---|
| Manage your Operational Resilience activities from the interactive dashboard in the Home page. | Exploring the Home page | Operational Resilience managers and users |
| Monitor your individual and team tasks from a single dashboard in the **My tasks** view. | Exploring the Tasks page and List page | Operational Resilience managers and users |
| Set up your business services in Operational Resilience workspace. | Setting up your business services in Operational Resilience Workspace | Operational Resilience managers and users |
| Analyze the importance and impact tolerance of a business service. | Analyzing the importance and impact tolerance of a business service in Operational Resilience Workspace | Operational Resilience managers and users |
| Perform a scenario analysis in Operational Resilience workspace. | Performing a scenario analysis in Operational Resilience Workspace | Operational Resilience managers and users |
| Self-attest the business services in Operational Resilience workspace. | Self-attesting the business services in Operational Resilience Workspace | Operational Resilience managers and users |
| Associate an issue in Operational Resilience workspace. | Associating an issue in Operational Resilience Workspace | Operational Resilience managers and users |

## Configuring Operational Resilience

Configure the Operational Resilience application to identify risks, strengthen controls, monitor services and processes, and ensure a complete resilience of your organization.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Operational Resilience configuration overview

Configuring Operational Resilience involves installing the application from ServiceNow® Store and setting it up by the administrators.

A typical configuration of the Operational Resilience application consists of the following steps:

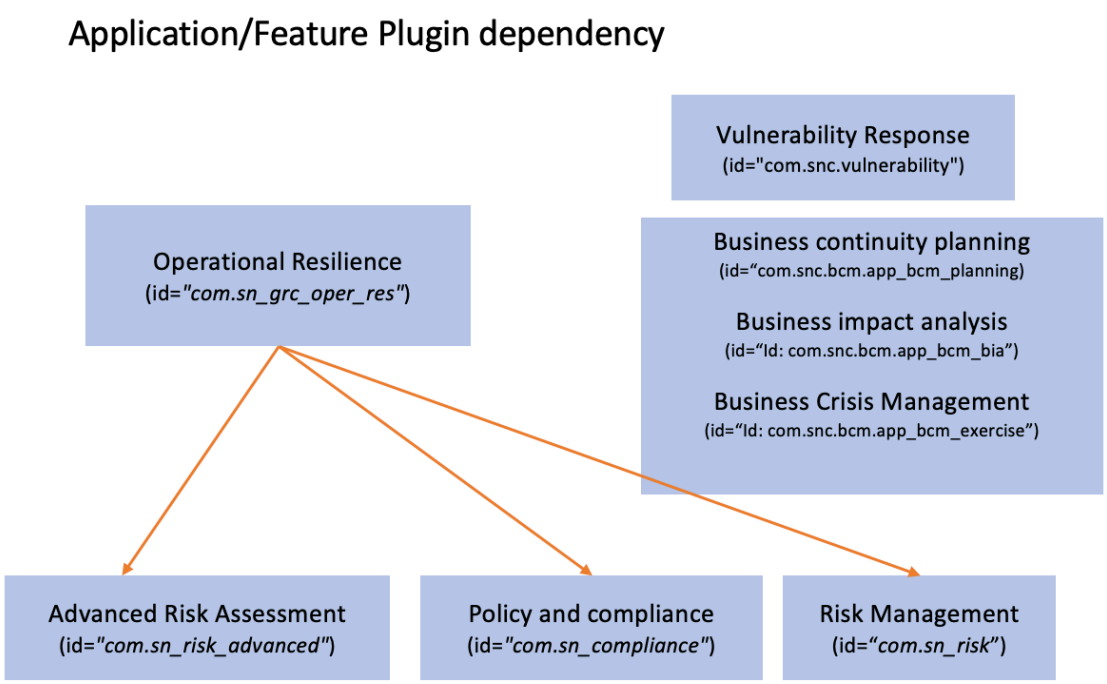
- Review the pre-requisites for Operational Resilience. For more information, see Pre-requisites for Operational Resilience.
- Download the Operational Resilience application from the ServiceNow Store. For more information, see Download Operational Resilience application.
- Perform the administrative setup tasks. For more information, see Setting up the administrative tasks.

## Pre-requisites for Operational Resilience

Before you install the Operational Resilience application, you must install the required GRC applications in your instance.

The following example shows the Operational Resilience hierarchy, required GRC applications, and optional GRC applications that you can add to the reporting dashboard.

### Operational Resilience application hierarchy




The Operational Resilience application (com.sn_grc_oper_res) requires that the following required applications be downloaded:

- GRC: Advanced Risk
- GRC: Policy and Compliance Management
- GRC: Risk Management

You can integrate GRC: Operational Resilience with the following optional applications:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- GRC: Business Continuity Management
- GRC: Vulnerability Response

Depending on the applications installed in your instance, you can view the reports on the Operational Resilience reporting dashboard.

## Download Operational Resilience application

Download the GRC: Operational Resilience application from the ServiceNow Store and run it in your instance.

### Before you begin

Role required: sn_oper_res.admin

### Procedure

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

Related topics

List of plugins

## Setting up the administrative tasks

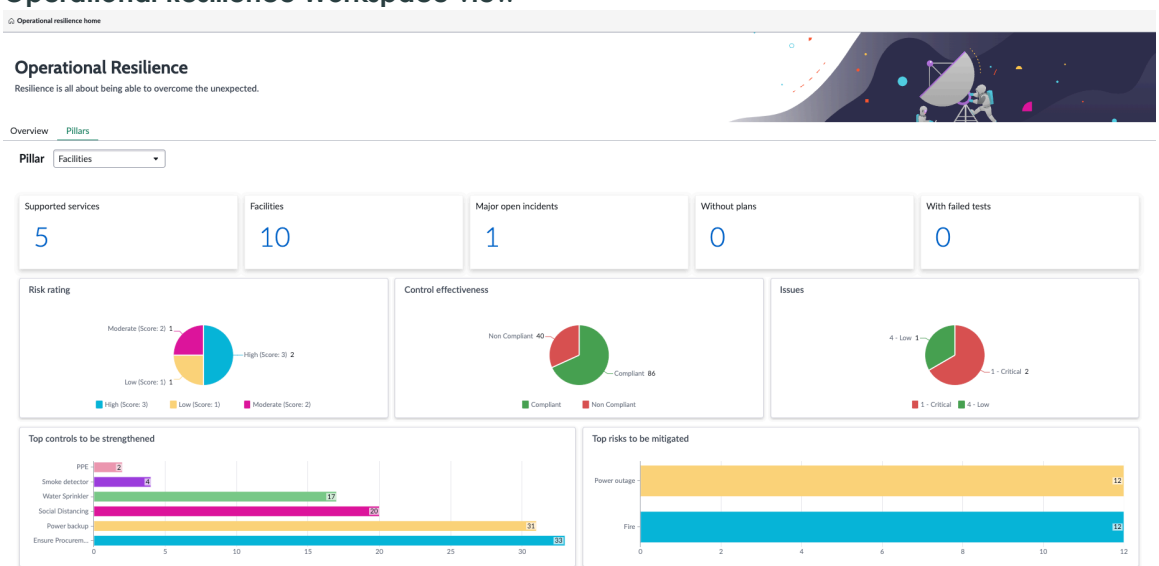
A user with the sn_oper_res.admin role can perform the setup tasks in the Operational Resilience application.

## Classic Operational Resilience and Operational Resilience Workspace

Prior to the Utah release, the Operational Resilience application supported the classic user interface. Beginning with the Utah release, the Operational Resilience application supports Operational Resilience Workspace.

Operational Resilience Workspace is a collection of tasks and workflows in a single focused working area. It enables you to configure multiple features in a single-pane view as shown in the following example.

### Operational Resilience Workspace view

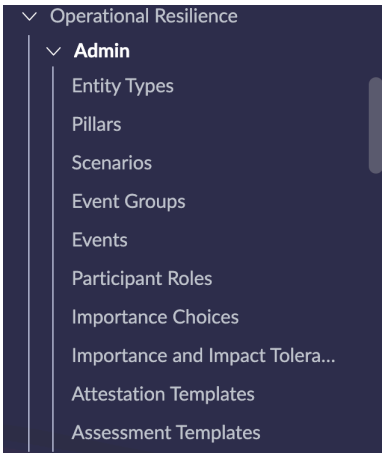



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Admin module in the classic Operational Resilience view

If you have the sn_oper_res.admin role, you can configure the Admin module by using the classic Operational Resilience application view as shown in the following example:

**Admin module in the classic view**




A user with the sn_oper_res.admin role can set up the following entities by using the Admin module:

- Entity Types
- Pillars
- Scenarios
- Event Groups
- Events
- Participant Roles
- Important Choices
- Importance and Impact Tolerance Rating Scale
- Attestation Templates
- Assessment Templates

**Note:** When you log in to the application as a user with the sn_oper_res.admin role, you can view the Admin module.

Operational Resilience administrators can create pillars and can also modify the reports on the dashboard.

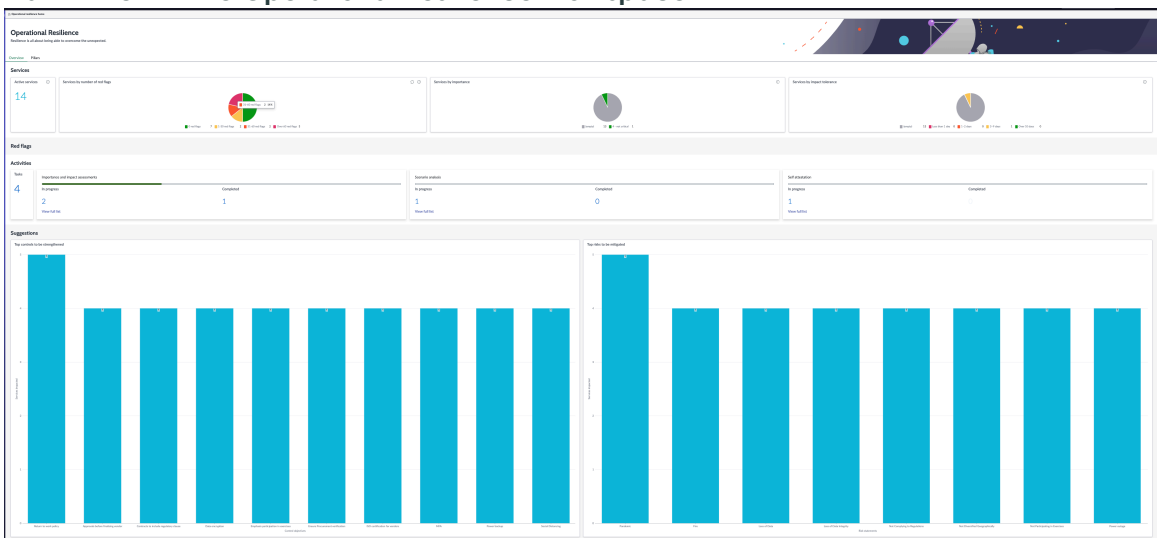
**Note:** Though you can modify the entity types, their filters, and pillars as a user with the sn_oper_res.admin role, you must exercise proper caution while modifying these entities.

## Admin view in Operational Resilience Workspace

If you have the sn_oper_res.admin role and you have the Utah release available in your instance, you can set up the admin view in Operational Resilience Workspace as shown in the following example:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Admin view in the Operational Resilience Workspace




## Administrative setup tasks

A user with the sn_oper_res.admin role can set up the following entities by using the Admin module:

- Entity Types
- Pillars
- Scenarios
- Event Groups
- Events
- Participant Roles
- Important Choices
- Importance and Impact Tolerance Rating Scale
- Attestation Templates
- Assessment Templates

**Note:** When you log in to the application as a user with the sn_oper_res.admin role, you can view the Admin module in the classic view or the admin view in Operational Resilience Workspace.

Operational Resilience administrators can create pillars and can also modify the reports on the dashboard.

**Note:** Though you can modify the entity types, their filters, and pillars as a user with the sn_oper_res.admin role, you must exercise proper caution while modifying these entities.

As a user with the sn_oper_res.admin role, you can complete the following setup tasks:

- Assign the Operational Resilience roles. For more information, see Assign Operational Resilience roles to your users.
- Set up an entity type to define data for a business entity. For more information, see Set up an entity type to define data for a business entity.
- Set up a pillar to define the core areas for your business. For more information, see Set up a pillar to define the core areas for your business entity.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Verify the setup checklist. For more information, see Verify the setup checklist.
- Create an event that you can associate with a scenario. For more information, see Create an event for your scenario.
- Classify an event by associating it with an event group. For more information, see Create an event group for your scenario.
- Create a scenario that represents a risk. For more information, see Create a scenario that you can associate with an event.
- Add a participant role for your scenario analysis. For more information, see Add a participant role for your scenario analysis.
- Update the assessment rating by using the Important choices module. For more information, see Update the assessment rating in the Important choices module.
- Update the importance and impact rating scale. For more information, see Set up the Importance and Impact Tolerance Rating Scale.
- Create an attestation template. For more information, see Create and edit an attestation template.

### Assign Operational Resilience roles to your users

Assign the appropriate roles to the users of the Operational Resilience application.

#### Before you begin
Role required: sn_oper_res.admin

#### About this task
To use the Operational Resilience application successfully, you must assign relevant roles to your users.

#### Procedure
1. Navigate to **All** > **User Administration** > **Users**.
2. Click the name of a user.
3. Click the **Roles** tab.
4. Click **Edit**.
5. Move the roles that you want to assign to the user from the Collection side to the Roles List and click **Save**.
6. Repeat these steps for each of your users.
   For more information on the roles, see Roles installed with Operational Resilience.

### Set up an entity type to define data for a business entity

Set up an entity type in the Operational Resilience application so that you can define the data for a business entity.

#### Before you begin
Role required: sn_oper_res.admin

#### About this task
An entity in Governance, Risk, and Compliance can be a person, a process, a department, an application, or an object. An entity type in Governance, Risk, and Compliance is a group of the entities that have similar attributes.

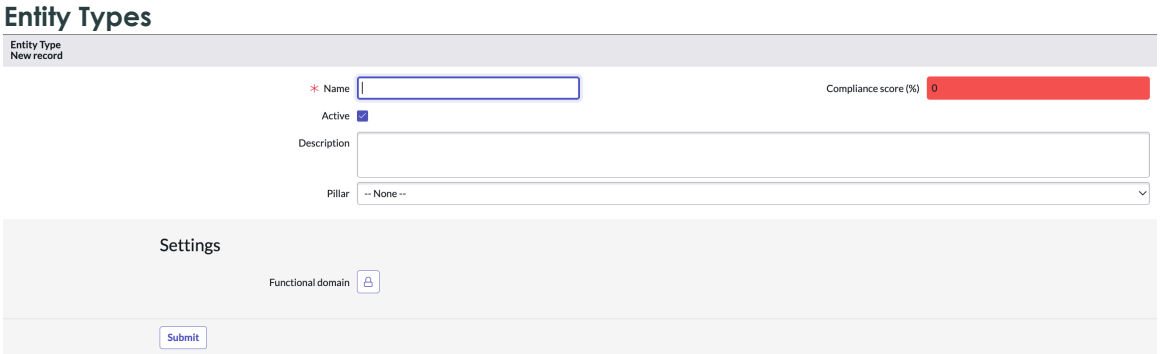
The entity type form in the Operational Resilience application is pre-configured with an entity filter that defines the data for an entity.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can use the pre-defined entity types that are provided with the base system or you can create an entity type depending on your business requirement. You can operate Operational Resilience by using these entity types as shipped, edit them as needed, or create entity types.

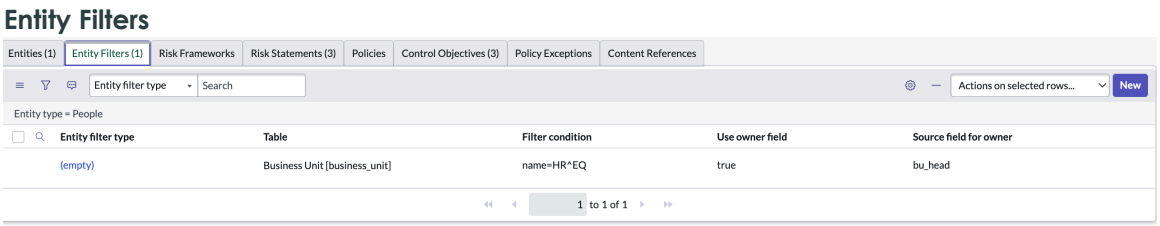
## Procedure

1. Navigate to **All** > **Operational Resilience** > **Admin** > **Entity Types**.




Each of the entity type includes an entity filter.

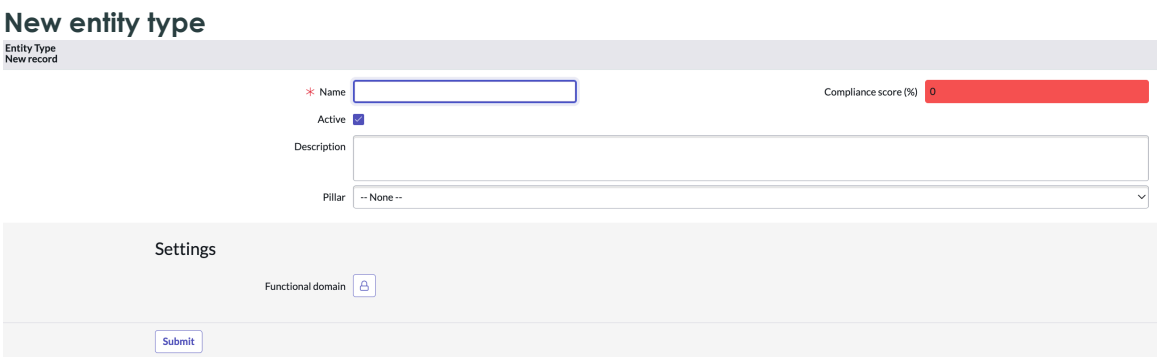
2. Click the **Name** of an entity type and click the Entity Filters tab to view its filter.




The entity filter is used to define the table from which data is to be pulled into each entity type for display in the Operational Resilience application.

**Note:** With the given default entity types, Facilities, People, Suppliers, Services, Processes, and Technology are used to pull data into the pillars.

3. To create an entity type, return to the Entity Types screen, and click **New**.




4. On the form, fill in the fields.
   For a description of the field values, see Entity Type New record form.
5. Click **Submit**.
   The newly defined entity type is listed in the Entity Types screen.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Entity Type New record form

Use the Entity Type New record form to create an entity type depending on your business requirement.

## Entity Type New record form

For a description of the field values, see the following table.

**Entity Type New record form**

| Field | Description |
|---|---|
| Name | Name of the entity type such as Business Processes, Services, or Facilities. |
| Compliance Score Percentage | Compliance score percentage for the entity type as defined in the Policy and Compliance Management application. Auto-populated field. |
| Active | Option to mark the entity type as active. |
| Description | Description for the entity type. |
| Pillar | Category that is used to organize your risk data and that an entity type is assigned to. The available options are as follows:<br>• **Services**<br>• **Process**<br>• **Suppliers**<br>• **Technology**<br>• **Facilities**<br>• **People** |
| Settings | |
| Functional domain | Functional domain for the entity, for example, IT and risk compliance. |

### Set up a pillar to define the core areas for your business entity

Set up a pillar in the Operational Resilience application so that you can define the core areas for your business entity.

#### Before you begin

Role required: sn_oper_res.admin

#### About this task

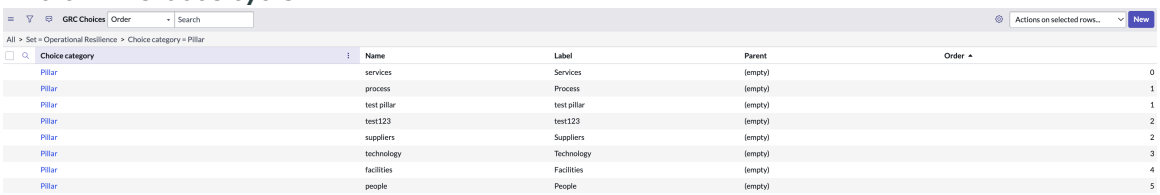
The Operational Resilience base system includes the pre-defined pillars such as Technology, Facilities, People, Services, Processes, and Suppliers. You can create a pillar or use the pre-defined pillar for your business requirement.

#### Procedure

1. Navigate to **All** > **Operational Resilience** > **Admin** > **Pillars**.
   The following example shows the pillars in the base system. For each of the pillars, a default entity type is included in the base system.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

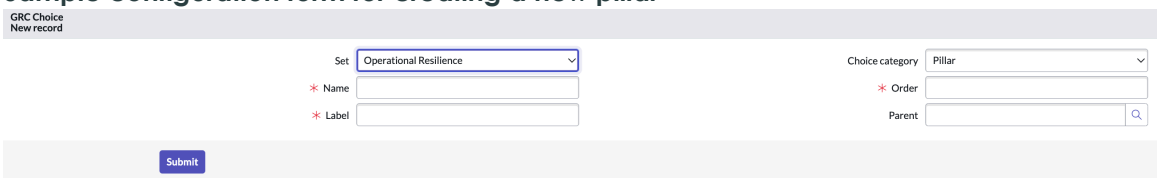
**Pillars in the base system**




For example, the Technology pillar comes with the Technology entity type pre-selected.

2. To create a pillar, click **New**.

**Sample configuration form for creating a new pillar**




3. On the form, fill in the fields.
   For a description of the field values, see GRC Choices form.
4. Click **Submit**.

### GRC Choices form

Use the GRC Choices form to set up a pillar to define the core areas for your business entity.

## GRC Choices form

For a description of the field values, see the following table.

**GRC Choices form**

| Field | Description |
|---|---|
| Set | View that is set to Operational Resilience. |
| Name | Name that the pillar belongs to such as Process, Suppliers, Technology, Facilities, People, Services, and Processes. |
| Label | Label for the pillar that is displayed in the UI. |
| Choice category | Category that is set to **Pillar** by default. |
| Order | Order for the pillar. |
| Parent | Parent entity that is associated with the selected pillar. |

### Create an event for your scenario

Create an event in the Operational Resilience application so that you can associate it with a scenario and assess its impact on your services.

**Before you begin**
Role required: sn_oper_res.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

If you have the sn_oper_res.admin role, you can create an event in the Operational Resilience application. An event can be something like flooding or a power outage. You can classify the events that are of a similar type under an event group.

### Procedure

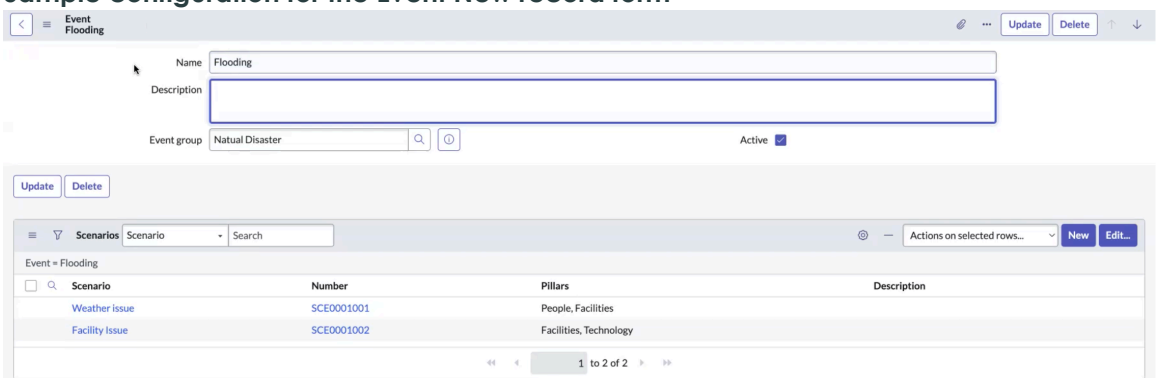
1. Navigate to **All** > **Operational Resilience** > **Admin** > **Events**.
2. Click **New**.
3. In the **Name** field, enter the name for the event.
4. In the **Description** field, enter the description for the event.
5. In the **Event group** field, select an event group.

   For a description of the field values in the form, see Event New record form.

   **Note:** You can add an event to many scenarios, but you can add an event to a scenario only once.

6. Click **Submit**.
   You can classify an event under an event group as shown in the following example.

**Sample configuration for the Event New record form**




As shown in the example, the scenarios for an event can be associated with different pillars.

### Event New record form

Use the Event New record form to create an event that you can associate with a scenario and assess its impact on your services.

## Event New record form

For a description of the field values, see the following table.

**Event New record form**

| Field | Description |
|---|---|
| Name | Name of the event. For example, Flooding or Earthquake. |
| Description | Description of the event. |
| Event group | Event group that you associate with the event. For example, Weather Issues. |
| Active | Option to mark the event as active. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create an event group for your scenario

Create an event group in the Operational Resilience application so that you can categorize the events that are defined in a scenario.

## Before you begin

Role required: sn_oper_res.admin

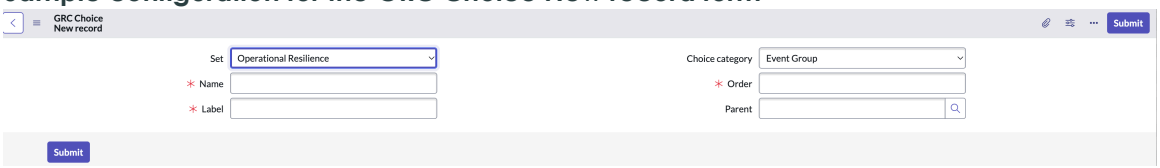
## About this task

Classify the events of a similar type into an event group for your scenario. For example, you can classify a natural event, such as flooding, into the Weather event group. Similarly, you can classify a power outage under the Energy Issues event group.

## Procedure

1. Navigate to **All** > **Operational Resilience** > **Admin** > **Event Groups**.
2. Click **New**.
3. In the **Name** field, enter the name for the event group.
4. In the **Label** field, enter the label for the event group.
   The configuration of a sample event group is shown in the following example.

**Sample configuration for the GRC Choice New record form**




5. In the **Order** field, enter the order for the event group and click **Submit**.
   For more information on the fields in the Event group form, see GRC Choice New record form.

### GRC Choice New record form

Use the GRC Choice New record form to classify your events and organize them into event groups.

## GRC Choice New record form

For a description of the field values, see the following table.

**GRC Choice New record form**

| Field | Description |
|---|---|
| Set | View that is set to Operational Resilience by default. |
| Name | Name of the event group. For example, Weather or Energy Issues. |
| Label | Label for the event group that appears in the UI. |
| Choice category | Category that is set to **Event group** by default. |
| Order | Order of the event group. |
| Parent | Parent category that you associate with an event group. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Create a scenario that you can associate with an event

Create a scenario in the Operational Resilience application so that you can associate it with an event and assess its impact on your business services.

### Before you begin

Role required: sn_oper_res.admin

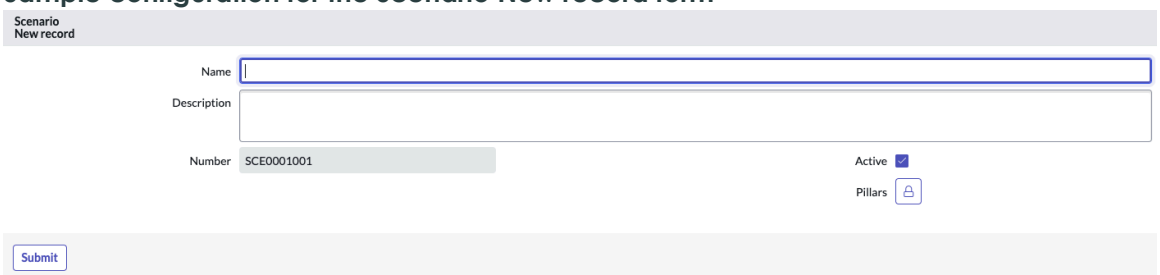
### About this task

A scenario helps you to determine the risks that are applicable to your business. If you have the sn_oper_res.admin role, you can create a scenario in the Operational Resilience application. You can use a scenario to test how an event can impact your organization.

### Procedure

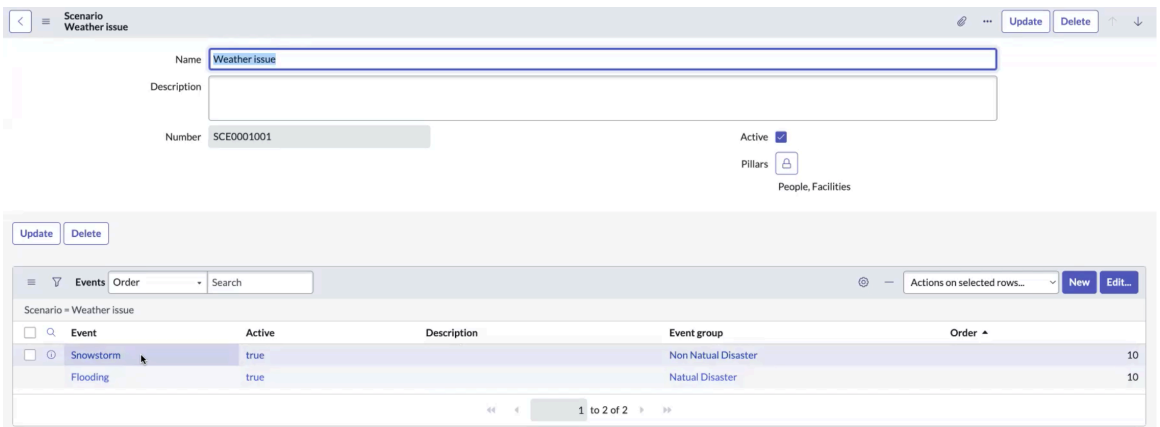
1. Navigate to **All** > **Operational Resilience** > **Admin** > **Scenarios**.
2. Click **New**.
   The sample configuration for the Scenario New record form is shown in the following example.

**Sample configuration for the Scenario New record form**




3. On the form, fill in the fields.
   For the description of the field values, see Scenario New record form.
4. Click **Submit**.
   You have associated an event with a scenario. The Events related list displays the associated events as shown in the following example.

**Events that are associated with a scenario**




   The order for the event is tied to the scenario and it is auto-filled by default in the related list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Scenario New record form

Use the Scenario New record form to create a scenario and test how an event that is associated with a scenario can impact your organization.

## Scenario New record form

For a description of the field values, see the following table.

**Scenario New record form**

| Field | Description |
|---|---|
| Name | Name of the scenario. |
| Description | Description of the scenario. |
| Number | Number of the scenario record. This field is auto-filled. |
| Active | Option to mark the scenario as active. |
| Pillars | List of pillars that you can associate with the scenario. The following pillars are provided with the Operational Resilience base system:<br>• Facilities<br>• People<br>• Process<br>• Suppliers<br>• Technology |
| Related list (Displayed after a scenario is added) | |
| Events | Events that are related to a scenario. The related list displays the name of the event, its active status, description, associated event group, and its order that is related to the scenario. The order for the event is tied to the scenario and it is auto-filled by default in the related list.<br>**Note:** You can add a new event or edit an existing event that is related to a scenario. |

### Verify the setup checklist

Verify the setup checklist in your instance so that you can complete the configuration tasks and prepare the Operational Resilience base system ready for the usage.

#### Before you begin

Role required: sn_oper_res.admin

#### About this task

Optional setup procedures are also included to enhance the GRC: Operational Resilience functionality.

#### Procedure

1. Verify that you have the GRC core applications installed on a Now Platform instance.

   **Note:** The GRC applications and the Now Platform instance should be from the same family release.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- To verify the GRC: Profiles application is installed on your instance, navigate to **Plugins** and search for GRC: Profiles.
- If the GRC: Profiles core application is not already installed, click **Install** to install it.
- Install the GRC: Advanced Risk, GRC: Risk Management, and GRC: Policy and Compliance Management applications.
- After these applications have been installed, install the Operational Resilience application.

If the applications listed in this step are not visible in your instance, the GRC core applications are available from the ServiceNow Store.

For more information about getting the entitlement, downloading, and installing the GRC core applications, see GRC and the ServiceNow Store.

2. Verify that you have assigned the required roles to your users.
   For detailed instructions and a list of Operational Resilience roles, see Assign Operational Resilience roles to your users.
3. Use the entity types included in the Operational Resilience base system, along with predefined entity filters.
   The entity filters define the data to be displayed on the dashboard. You can operate Operational Resilience using these entity types as shipped, edit them as needed, or create entity types. For detailed instructions, see Set up an entity type to define data for a business entity.
4. Use the pillars included in the base system.
   You can operate Operational Resilience using these pillars as shipped, edit them as needed, or create pillars. For detailed instructions, see Set up a pillar to define the core areas for your business entity.
5. To generate a PDF, click the **Save As PDF** icon ( ) at the top of the topic and click **Selected topic**.
   You can create and print a PDF of the steps. You can then check off tasks as you complete them.

### Result

After completing the steps listed in this section, you have successfully set up the GRC: Operational Resilience base system. You can customize many of the elements included in the base system for your particular business needs. Refer to the links in the steps for more information.

## Add a participant role for your scenario analysis

Add a participant role for your scenario analysis in the Operational Resilience application so that you can collect the observations and recommendations of the participants by their roles and functions.

### Before you begin

Role required: sn_oper_res.admin

### About this task

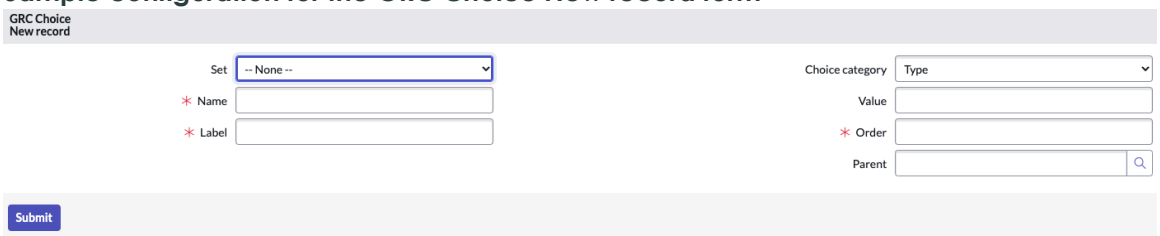
Depending on the scenario analysis type, such as a scenario analysis for critical services, you can add the participants from the associated business functions and assign various roles. For example, you can add HR, Legal, Finance, or Procurement roles to your participants.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Operational Resilience** > **Admin** > **Participant Roles** and click **New**.
2. In the **Set** field, select **Operational Resilience**.
3. In the **Name** field, enter the name for the participant role.
4. In the **Label** field, enter a label for the participant role.
5. In the **Choice category** field, select **Role**.
6. In the **Value** field, enter the value of the choice for the participant role.
7. In the **Order** field, enter an order for the participant role.
   This field displays the order of the participant role in the GRC Choice table.
8. In the **Parent** lookup list options, select a parent service.
   See the sample configuration for a participant role as shown in the following example.

**Sample configuration for the GRC Choice New record form**




9. Click **Submit**.

### Result

In the Participant Roles module in the application UI, the participant role is listed in the Roles list view.

#### GRC Choice New record form

Use the GRC Choice New record form to add a role for the participants of your scenario analysis.

## GRC Choice New record form for the role

For a description of the field values, see the following table.

**GRC Choice New record form**

| Field | Description |
|---|---|
| Set | View that is set to Operational Resilience by default. |
| Name | Name of the role. For example, Facilities or Finance. |
| Label | Label for the role that appears in the UI. |
| Choice category | Category that is set to **Role** by default. |
| Value | Integer value that you set for the role. |
| Order | Order of the role. This field displays the order of the participant role in the GRC Choice table. |
| Parent | Parent category that you associate with the role. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Set up the Importance and Impact Tolerance Rating Scale

Set up the Importance and Impact Tolerance Rating Scale in the Operational Resilience application so that you can define new parameters for your business services.

### Before you begin

Role required: sn_oper_res.admin

### About this task

Define new parameters such as importance, impact tolerance, impact tolerance icon and its color, minimum and maximum tolerance value, and the tolerance order for your business service. When the options in the sn_grc_choice table are set as *choice_category=opres_asmt_rating* and *set=operational_resilience*, the Operational Resilience application delivers the following default importance rating scales. This task is optional.

#### Default importance rating scales

| Importance | Impact tolerance | Impact tolerance icon | Minimum-maximum score | Order |
|---|---|---|---|---|
| 1—Most critical | 1 Day | flag-fill | 76—100 | 10 |
| 2— Somewhat critical | 2 Days | triangle-exclamation-fill | 51—75 | 20 |
| 3—Less critical | 3 Days | binoculars-fill | 26—50 | 30 |
| 4—Not critical | 4 Days | circle-check-fill | 0—25 | 40 |

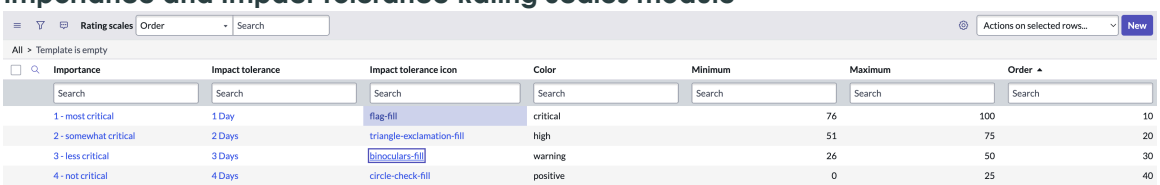
When a new questionnaire template is created, the application clones the default rating scale to it.

A user with the sn_oper_res.admin role can change the rating scale for the individual templates.

### Procedure

1. Navigate to **All** > **Operational Resilience** > **Admin** > **Importance and Impact Tolerance Rating Scale**.
   You see the default importance and impact tolerance rating scales as shown in the following example.

**Importance and Impact Tolerance Rating Scales module**




2. Click **New**.
   You can define new parameters such as the importance, impact tolerance, impact tolerance icon and its color, minimum and maximum tolerance value, and the tolerance order for your business service.
3. On the form, fill in the fields and click **Submit**.
   For a description of the field values on the Rating Scale New Record form, see Rating Scale New Record form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Rating Scale New Record form

Use the Rating Scale New Record form to set up the default importance rating scale to define the parameters of the rating scale for your business services.

## Rating Scale New Record form

For a description of the field values, see the following table.

**Rating Scale New Record form**

| Field | Description |
|---|---|
| Importance | Importance scale for the service. Available options are as follows:<br>• **1- Most critical**<br>• **2- Somewhat critical**<br>• **3- Less critical**<br>• **4- Not critical** |
| Color | Color for the selected tolerance rating. Available options are:<br>• none<br>• blue<br>• brown<br>• critical<br>• gray<br>• green<br>• green-yellow<br>• high<br>• info<br>• low<br>• magenta<br>• moderate<br>• orange<br>• pink<br>• positive<br>• purple<br>• teal<br>• warning<br>• yellow |
| Order | Order for the defined importance and tolerance duration. |
| Minimum | Minimum score for the tolerance level of the disruption. |
| Maximum | Maximum score for the tolerance level of the disruption. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Rating Scale New Record form (continued)

| Field | Description |
|---|---|
| Impact tolerance | Impact tolerance duration in days as per the defined importance of the service. |
| Impact tolerance icon | Impact tolerance icon for the selected tolerance rating. |

### Update the assessment rating in the Important choices module

Update the rating of the assessment in the Operational Resilience application so that you can update the criticality and the order of the assessment for your business services.

## Before you begin

Role required: sn_oper_res.admin

## About this task

You can update the criticality and the order of the assessment rating by using the Important choices module. This task is optional.

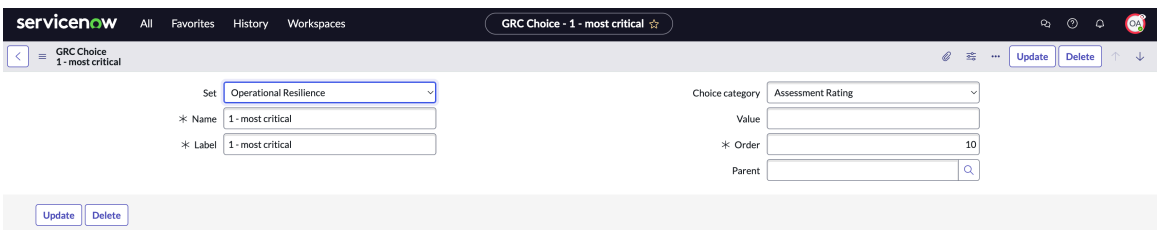
## Procedure

1. Navigate to **All** > **Operational Resilience** > **Admin** > **Important Choices**.
   You see the default assessment rating that is shown in the following example.

**Default assessment rating**




   A sample assessment rating is shown in the following example.




2. Click **New**.
3. On the form, fill in the fields and select **Submit**.
   For a description of the field values on the GRC Choices form, see GRC Choices form.

### GRC Choices form

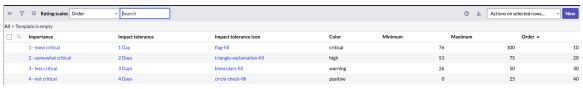
Use the GRC Choices form to set up the rating of the assessment by updating its criticality and the order of the choice in the Important choices module.

## GRC Choices form

For a description of the field values, see the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### GRC Choices form

| Field | Description |
|---|---|
| Set | View that is set to Operational Resilience. |
| Name | Name of the assessment rating. For example, **1- Most Critical**. |
| Label | Label of the assessment rating. For example, **1- Most Critical**. |
| Choice category | Choice category. It is set to **Assessment Rating** by default. |
| Order | Field used for sorting the order of the assessment rating. Based on the Importance and Impact Assessment score, the application selects the corresponding rating.  |
| Parent | Parent setting that is associated with the assessment rating. For example, the **Technology** pillar can be associated with the assessment rating. |

## Create a custom questionnaire template

Create your own questionnaire (assessment) template instead of using the default template in the Operational Resilience application to suit your business needs.

### Before you begin

Role required: sn_oper_res.admin

### About this task

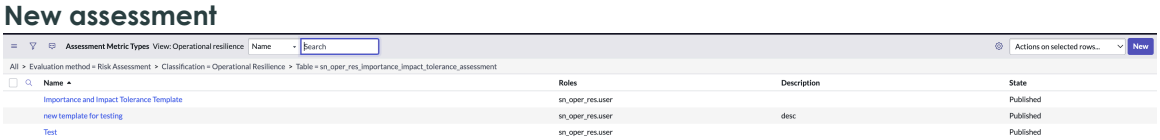
Create your own questionnaire (assessment) template and request the responses from the assessor. This task is optional.

### Procedure

1. Navigate to **All** > **Operational Resilience** > **Administration** > **Assessment Templates**.
2. To create an assessment template, click **New** as shown in the following example.




3. On the Assessment Metric Type form, fill in the fields and click **Submit**.
   The new assessment template is listed in the Assessment Metric Types list as shown in the following example.




For a description of the field values on the Assessment Templates form, see Assessment Metric Type form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Assessment Metric Type form

Use the Assessment Metric Type form to create an assessment questionnaire template instead of using the default template. You can also use this form to request responses from the assessor.

## Assessment Metric Type form

For a description of the field values, see the following table.

**Assessment Metric Type form**

| Field | Description |
|---|---|
| Name | Name of the assessment template. |
| Roles | Additional user roles that can view the results and access records that are associated with this template. Users with the specified roles have read access to this template record and to the associated categories, metrics, assessable records and scorecards, category users, stakeholders, and decision matrices. |
| Active | Option to enable the assessment template. |
| State | Status of the assessment: **Draft** or **Published**. This field is auto-filled. |
| Description | Helpful information about the assessment template. Enter a clear description of the template and its purpose. |

### Create and edit an attestation template

Create a customized attestation template in the Operational Resilience application that suits your business needs. By customizing an attestation template, you can add your own questions for your self-attestation. You can also edit an existing attestation template for your own business needs.

## Before you begin

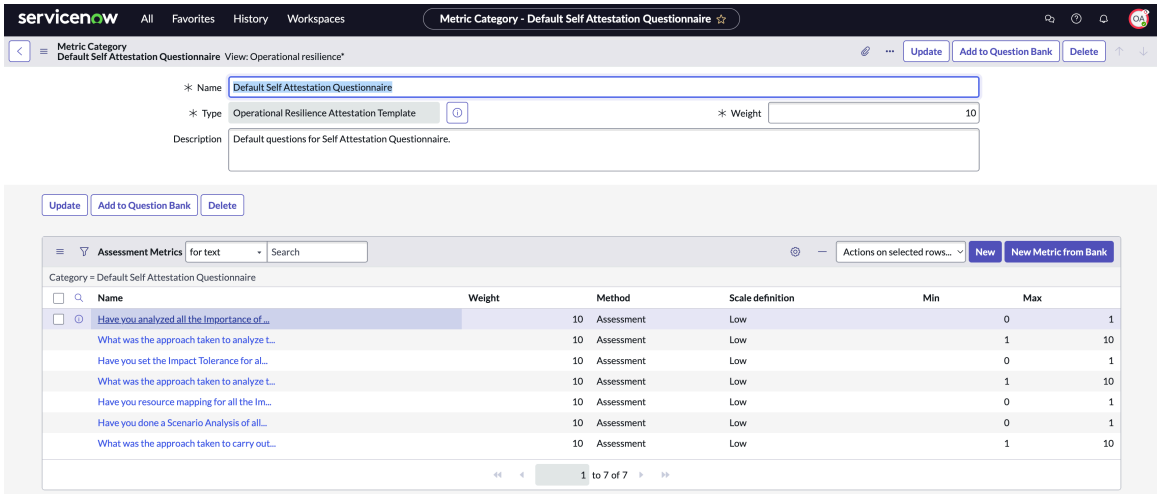
Role required: sn_oper_res.admin

## About this task

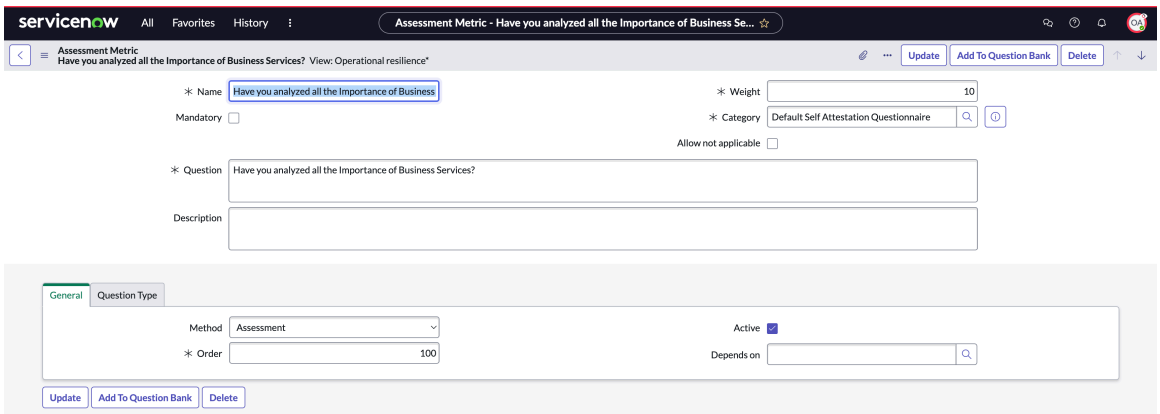
The Operational Resilience application provides you with an attestation template as part of the base system. Creating an attestation template is optional.

If you have the sn_oper_res.admin role, you can also edit an existing attestation template for your own business needs. You can select and update the questions in the attestation template as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

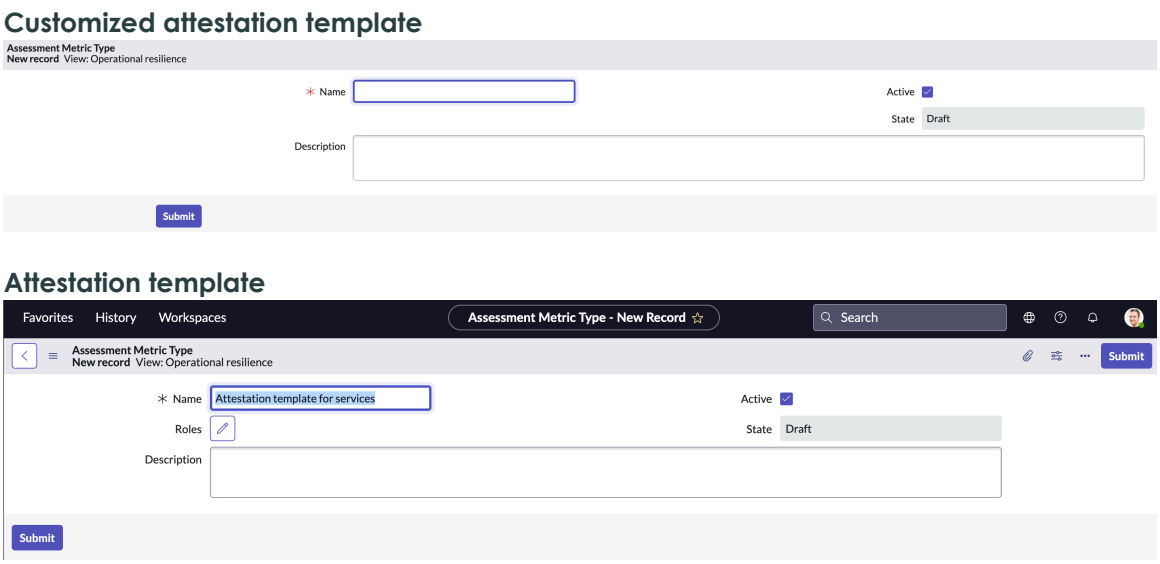



You can update the questions according to your business requirements as shown in the following example.




## Procedure

1. Navigate to **All** > **Operational Resilience** > **Administration** > **Attestation Templates**.
2. To create a customized template, select **New**.



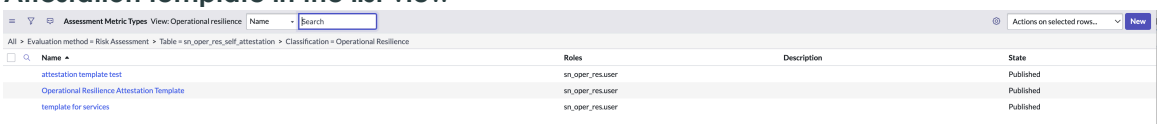

3. On the Assessment Metric Type New Record form, enter the name for the attestation template and select **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For a description of the field values on the form, see Assessment Metric Type New Record form.

The attestation template is displayed in the templates list view as shown in the following example.

**Attestation template in the list view**




By selecting **Submit**, you add the Operational Resilience tables and the application users to your customized attestation template.

### Assessment Metric Type New Record form

Use the Assessment Metric Type New Record form to create an attestation template to create the attestations. Use the template form to create a record.

## Assessment Metric Type New Record form

For a description of the field values on the form, see the following table.

**Assessment Metric Type New Record form**

| Field | Description |
|---|---|
| Name | Name of the template. |
| Description | Information about the template. |
| Active | Option to enable the template. |
| State | State of the assessment. The available options are as follows:<br>• **Draft**<br>• **Published**<br><br>This field is auto-filled. |

### Create a customized HTML document template

Create a customized HTML document template in the Operational Resilience application to suit your business needs. You can use the customized HTML document template instead of the default HTML template to export an attestation.

#### Before you begin

Role required: sn_oper_res.admin

#### About this task

Creating a customized HTML document template is optional.

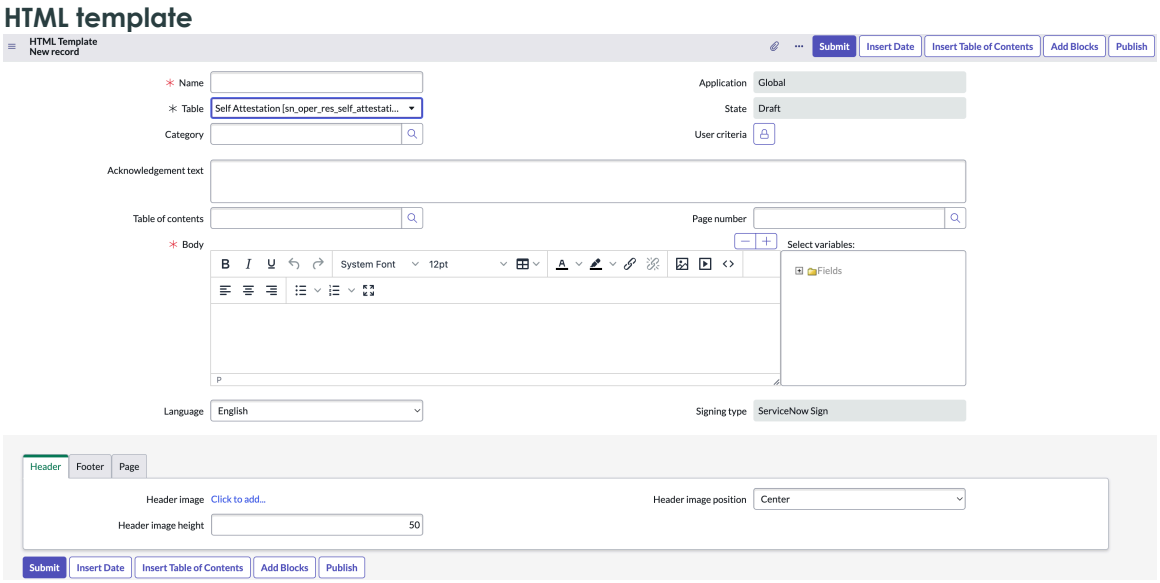
#### Procedure

1. Navigate to **All** > **Document Templates** > **All Document Templates** and click **New**.
   The following question is displayed on the form: *What kind of document template would you like to create?*The available options are as follows:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- HTML Document Template
- PDF Document Template

2. Select **HTML Document Template**.
3. In the **Table** field, select the **Self Attestation [sn_oper_res_self_attestation]** table.
   The sample form is shown in the following example.




4. On the form, fill in the fields and click **Submit**.
   The new template is displayed in the Document Templates list. For descriptions of the field values, see HTML Template form.

### Result

If you have the sn_oper_res.manager role, you can use the HTML template to generate a self-attestation report.

### HTML Template form

If you have the sn_oper_res.admin role, use the HTML Template form to create an HTML template instead of using the default HTML template.

## HTML Template form

For a description of the field values on the form, see the following table.

**HTML Template form**

| Field | Description |
|---|---|
| Name | Unique name for the HTML template. |
| Table | Type of table that is used for the template. The default value is the Self attestation [sn_oper_res_self_attestation] table. |
| Category | Category of the document template, such as Operational Resilience. |
| Application | Type of the application such as Global. This field is auto-filled. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**HTML Template form (continued)**

| Field | Description |
|---|---|
| State | State of the application such as Global. This field is auto-filled. |
| User criteria | Target record for the user criteria such as GRC Business Users. |
| Acknowledgment text | Acknowledgment text for the HTML template. |
| Page number | Page number for the HTML template such as Default. |
| Body | Body text for the HTML template. |
| Language | Language for the HTML template. The default is English. |
| Signing type | Signature type for the HTML template. |
| Related lists | |
| Header | Information about the header image. The options are as follows:<br>• **Header image**: Click to add a header image.<br>• **Header image position**: Position the header image by using the following options:<br>◦ **Left**: Align the header image on the left of the page.<br>◦ **Center**: Align the header image in the center of the page.<br>◦ **Right**: Align the header image on the right of the page.<br>• **Header image height**: Value of the header image height in pixels. |
| Footer | Information about the footer image. The options are as follows:<br>• **Footer image**: Click to add a footer image.<br>• **Footer image position**: Position the footer image by using the following options:<br>◦ **Left**: Align the footer image on the left of the page.<br>◦ **Center**: Align the footer image in the center of the page.<br>◦ **Right**: Align the footer image on the right of the page.<br>• **Footer image height**: Enter the value of the footer image height. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**HTML Template form (continued)**

| Field | Description |
|---|---|
| | • **Footer text**: Add a footnote on the document.<br>• **Footer text position**: Position the footer text by using the following options:<br>◦ **Left**: Align the footer text on the left of the page.<br>◦ **Center**: Align the footer text in the center of the page.<br>◦ **Right**: Align the footer text on the right of the page.<br>• **Vertical alignment**: Align the footer text by using the following options:<br>◦ **Above the footer image**: Align the footer text above the footer image.<br>◦ **Below the footer image**: Align the footer text below the footer image. |
| Page | Information about the page. The options are as follows:<br>• Page size: Size of the page. The available options are as follows:<br>◦ **A4**: A4 page size for the HTML template.<br>◦ **Letter**: Letter page size for the HTML template.<br>◦ **Legal**: Legal page size for the HTML template.<br>• **Top/Bottom margin**: Top and bottom margin dimensions for the page in pixels.<br>• **Left/Right margin**: Left and right margin dimensions for the page in pixels. |

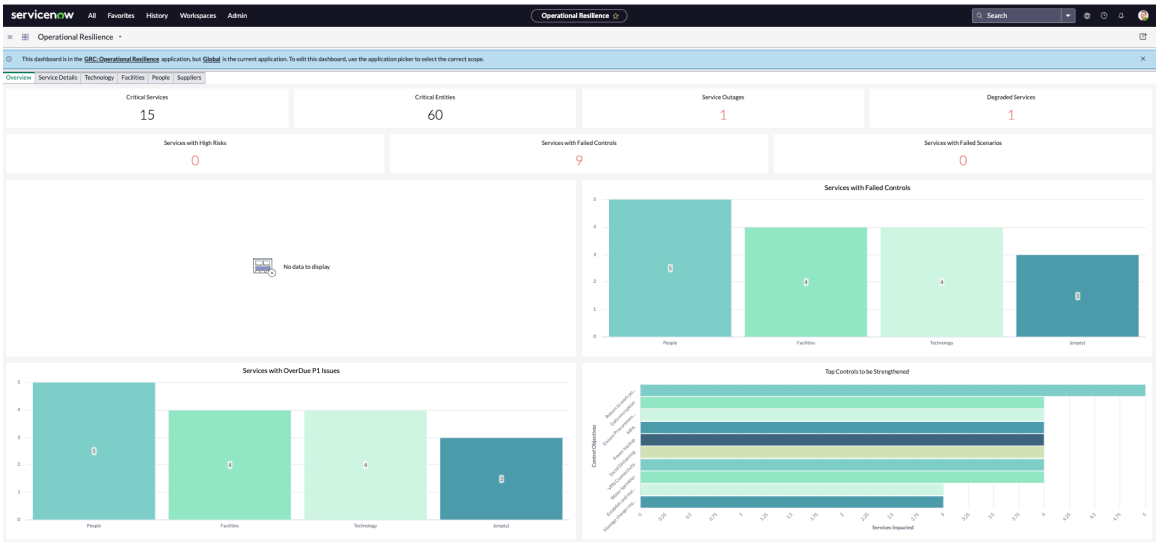
## Setting up the features and capabilities in classic Operational Resilience

Set up the features and capabilities of the Operational Resilience application in classic Operational Resilience. Monitor the reports on the dashboard and determine the overall resilience of your services.

After configuring the Operational Resilience application as explained in the previous section, you can set up the application to display an overview of your services. Set up the features and capabilities and view the reports for each pillar as shown in the following example.

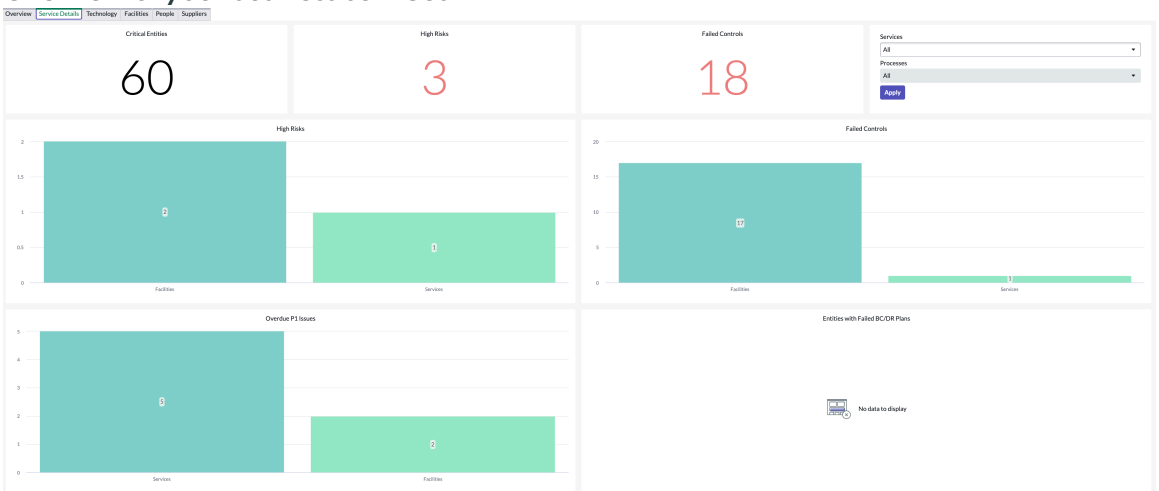
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Overview of the dashboard




Monitor the status of your business services by monitoring the overview tab as shown in the following example.

### Overview of your business services




In the Utah release, you can configure the following features and set up the reports on the Operational Resilience dashboard:

1. Analyze the importance and the duration of the impact tolerance of your business services. For more information, see Analyzing the importance and impact tolerance of the business services.
2. Perform a scenario analysis of your important business services. For more information, see Performing a scenario analysis of the business services.
3. Self-attest the status of your business services by submitting and generating the self-attestation report. For more information, see Self-attesting the status of the business services.

## Setting up the business services and their dependencies

The Operational Resilience application provides you with a business services view that consolidates the risks, issues, control failures, and other areas of your business services that need attention. You can set up the business services and their dependencies and monitor their operational resilience status on the reporting dashboard.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Overview of business services, parent services, and child services

A business service is a service that performs a business-level function. For example, you can use email, IT services, e-commerce, and telephone banking as business services that perform the business-specific functions in your organization.

You can classify a business service as a parent service and child service. A parent service is a broad entity that you can use to service a business function. A parent service may contain its own subentities. A child service inherits its properties from the parent service. For example, the Payments service is a parent service and Mortgage payment or Maintenance payment are its child services.

## Synchronizing the services and processes from the CMDB with Operational Resilience

In the Operational Resilience application, the parent services, child services, and processes are obtained from the Configuration Management Database (CMDB). The cmdb_rel_ci table in the CMDB maintains a relationship for the parent services, child services, and processes. You can associate a parent service, child service, or process to the current service by adding a relationship in the cmdb_rel_ci table.

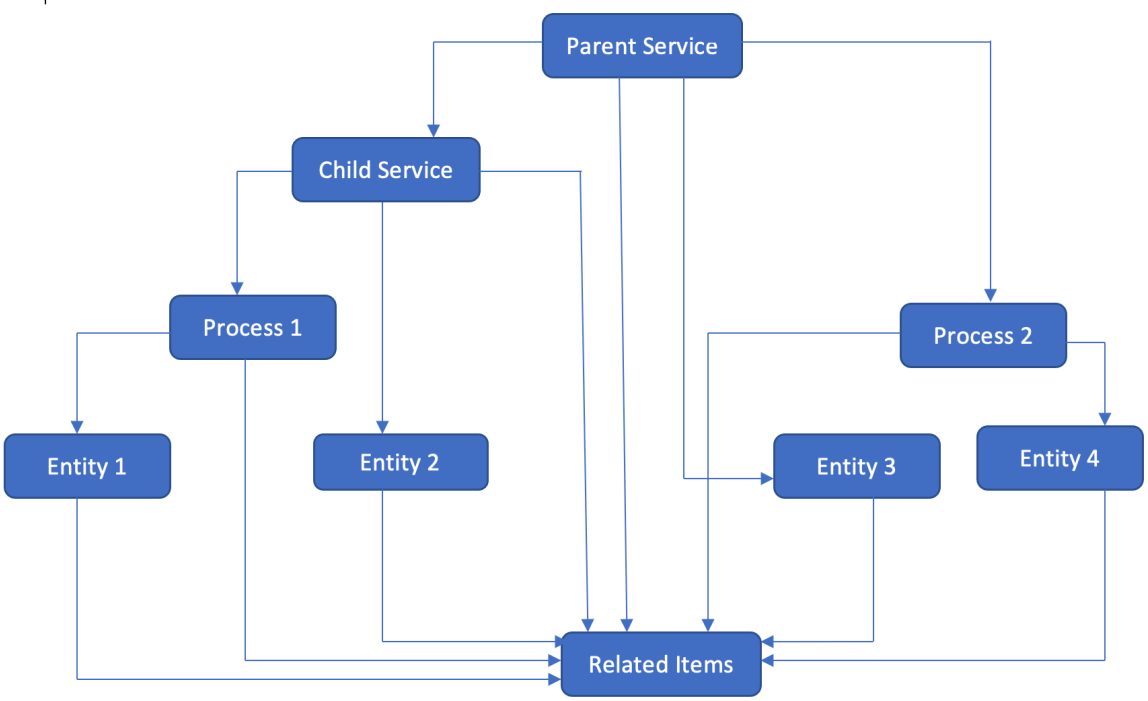
By default, the view is set to Operational Resilience in the Operational Resilience application. The view contains the cmdb_ci_service table with multiple related lists.

For information on the Configuration Management Database (CMDB), see Configuration Management Database (CMDB).

## Operational Resilience data architecture

To understand how the services, processes, and entities are connected in the Operational Resilience application, see the following example.

**Operational Resilience data architecture**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Operational Resilience application supports a data model that creates the business services and their dependencies as entities that are based on the entity types. You can use the Service entity type to scope the services that you want to monitor daily. Each service in the Service entity type is used to calculate its Operational Resilience data.

As shown in the example, the parent services and child services are associated with the business processes. Business processes are further associated with the assets known as the entities.

You can map your services and processes as explained in the following sample configuration:

1. Map your parent business services and child business services to their associated business processes.
2. Map the business processes to your pre-defined entities.
3. Map the services directly to the related lists (related items). A related item can be an entity, risk, risk assessment, control, incident, change request, outage, issue, or task.

As shown in the diagram, the Operational Resilience application synchronizes the relationship between the services and processes. Consider the following examples:

- When you add a parent service to a business service, an entity is automatically created for the added parent service. The new service entity is added to the upstream entity of the business service's entity.
- When you add a child service to a business service, an entity is automatically created for the added child service. The new service entity is added to the downstream entity of the business service's entity.
- When you add a child process to a business service, an entity is created for the child process. The new process entity is added to the downstream entity of the business service's entity.

## Pillars that are provided with the Operational Resilience base system

A pillar is a foundational block that contributes to the operational resilience of your organization. You can map your business services and processes to the pillars in the Operational Resilience application so that you can establish a relationship between these entities and monitor their status on the dashboard.

The Operational Resilience application provides the following pillars as part of the base system:

- Facilities
- People
- Suppliers
- Services
- Processes
- Technology

For more information on the pillars, see Exploring Operational Resilience.

The data that is associated with the pillars is displayed on the Operational Resilience dashboard. For example, the controls, risks, or P1 issues that are associated with an entity are displayed on the Operational Resilience dashboard.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you install the optional applications, such as Business Continuity Management and Vulnerability Response in your instance, you can also view the Business Continuity or Disaster Recovery plan and Vulnerability Response reports on the dashboard.

## Scheduled job that gathers the information from different applications

In Operational Resilience, the *Compute Operational Resilience Compliance* scheduled job runs in the background daily. It calculates its reports data by gathering the information from the following integrated applications:

- GRC: Advanced Risk
- GRC: Risk Management
- GRC: Policy and Compliance Management
- CMDB
- Business Continuity Management
- Vulnerability Response

For more information on the integrated applications for Operational Resilience, see Pre-requisites for Operational Resilience.

The scheduled job removes all the data from the previous day before creating the new supporting data for the reports. The job uses different inbuilt conditions to retrieve the data from different sources and saves it to the Operational Resilience staging tables.

The scheduled job generates the Operational Resilience controls, risks, issues, and outages for all the downstream entities of each entity within each entity type automatically.

## Information gathering for the services

The Operational Resilience application gathers the information from the different sources and conditions for the services. The following table describes the service modules in the Operational Resilience, their source applications, source tables, and filtering conditions that are used to populate the reports on the dashboard.

**Services modules and their source applications, source tables, and filtering conditions**

| Services Modules | External source application | Source table and filtering conditions |
|---|---|---|
| Parent Services | CMDB | Service [cmdb_ci_service]<br><br>Business criticality = 1 – most critical and Service Classification = Business Service |
| Child Services | CMDB | Service [cmdb_ci_service]<br><br>Business criticality = 1 – most critical and Service Classification = Business Service |
| Processes | CMDB | Service [cmdb_ci_service] |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Services modules and their source applications, source tables, and filtering conditions (continued)**

| Services Modules | External source application | Source table and filtering conditions |
|---|---|---|
| Assets | GRC: Profiles | Entity [sn_grc_profile]<br><br>The entity must be downstream of any business process entity of any service entity. |
| Services with Priority 1 Issues | Policy and Compliance Management | Issue [sn_grc_issue]<br><br>Priority = 1 - Critical and Active = true |
| High Risks | Advanced Risk Assessment | Risk Assessment [sn_risk_advanced_risk_assessment_instance]<br><br>The residual risk for the risk assessment is the highest defined in the qualitative rating criteria for the residual risk assessment type. |
| Failed Controls | Policy and Compliance Management | Control [sn_compliance_control]<br><br>Status = Non-compliant and State = Monitor |
| Services with Change Requests | CMDB | Change request (sn_oper_res_change_request): Change request created for the application. |
| Services with Tasks | CMDB | Task (sn_oper_res_task): Task defined in the application. |
| Services with Incidents | Incident Management | Incident [incident]<br><br>Service = one of the critical services and State is New, In progress, and On hold. |
| Services under Outage | CMDB | Affected CIs [cmdb_outage_ci_mtom]<br><br>Any downstream CI of any critical service that is under outage. |
| Importance and Impact Assessment | Not applicable | Service Impact Analysis [sn_oper_res_service_impact_analysis] |
| Scenario Analysis | Not applicable | Scenario Analysis [sn_oper_res_scenario_analysis_service] |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Services modules and their source applications, source tables, and filtering conditions (continued)**

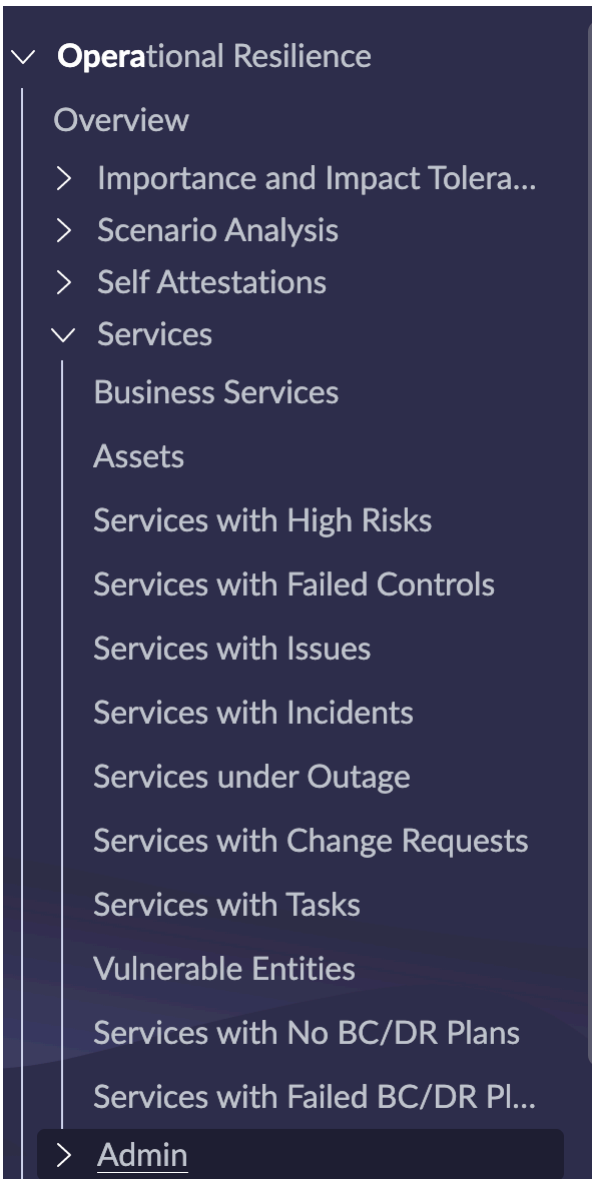
| Services Modules | External source application | Source table and filtering conditions |
|---|---|---|
| Vulnerable Entities | Vulnerability Response | Vulnerable Item [sn_vul_vulnerable_item]<br><br>Vulnerability field is not empty and the State is not Resolved, Deferred, or Closed. |
| Services with No BC/DR Plans | Business Continuity Management | Plan [sn_bcp_plan]<br><br>State = Approved and the plan is not expired. |
| Services with Failed BC/DR Plans | Business Continuity Management | Event [sn_recovery_event]<br><br>Event state = Exercise in the Closed Complete or Closed Incomplete state. The Result is Unsuccessful, and the associated plan is not expired. |

## Viewing the services in Operational Resilience

If you have the sn_oper_res.manager role, you can view the Services module by navigating to the **All** > **Operational Resilience** > **Services** module as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Services module**




As explained in the earlier section, you can view the services that are listed under the Services module depending on the applications that you have installed in your instance. The following services are listed in the Operational Resilience application view:

- Business Services
- Assets
- Services with High Risks
- Services with Failed Controls
- Services with Issues
- Services with Incidents
- Services under Outage
- Services with Change Requests
- Services with Tasks
- Vulnerable Entities

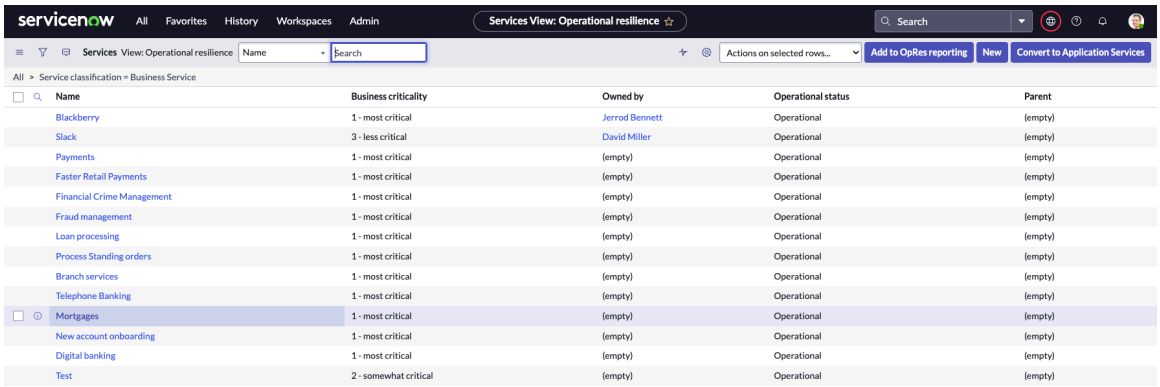
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Services with No BC/DR Plans
- Services with Failed BC/DR Plans

## Business services list view

When you click the Business Services module in the application navigator, you can view or update the associated services in the Business Services list view as shown in the following example.

**Business services list view**




| Name | Business criticality | Owned by | Operational status | Parent |
|---|---|---|---|---|
| Blackberry | 1 - most critical | Jerrod Bennett | Operational | (empty) |
| Slack | 3 - less critical | David Miller | Operational | (empty) |
| Payments | 1 - most critical | (empty) | Operational | (empty) |
| Faster Retail Payments | 1 - most critical | (empty) | Operational | (empty) |
| Financial Crime Management | 1 - most critical | (empty) | Operational | (empty) |
| Fraud management | 1 - most critical | (empty) | Operational | (empty) |
| Loan processing | 1 - most critical | (empty) | Operational | (empty) |
| Process Standing orders | 1 - most critical | (empty) | Operational | (empty) |
| Branch services | 1 - most critical | (empty) | Operational | (empty) |
| Telephone Banking | 1 - most critical | (empty) | Operational | (empty) |
| Mortgages | 1 - most critical | (empty) | Operational | (empty) |
| New account onboarding | 1 - most critical | (empty) | Operational | (empty) |
| Digital banking | 1 - most critical | (empty) | Operational | (empty) |
| Test | 2 - somewhat critical | (empty) | Operational | (empty) |

The Business Service list view shows the details for each service. For example, you can see the name, business criticality, its owner, operational status, and the related parent service.

## Adding a business service in Operational Resilience

If you have the sn_oper_res.manager role, you can add a service in the Operational Resilience application in one of the following ways in the Business services list view:

- You can select multiple services in the Business Services module and click **Add to OpRes reporting**.
- In the service record, you can click **Add to OpRes reporting**.
- You can use the Services related list to associate a service with the current service.

When you add a business service in Operational Resilience, the application populates the information on the service from the CMDB.

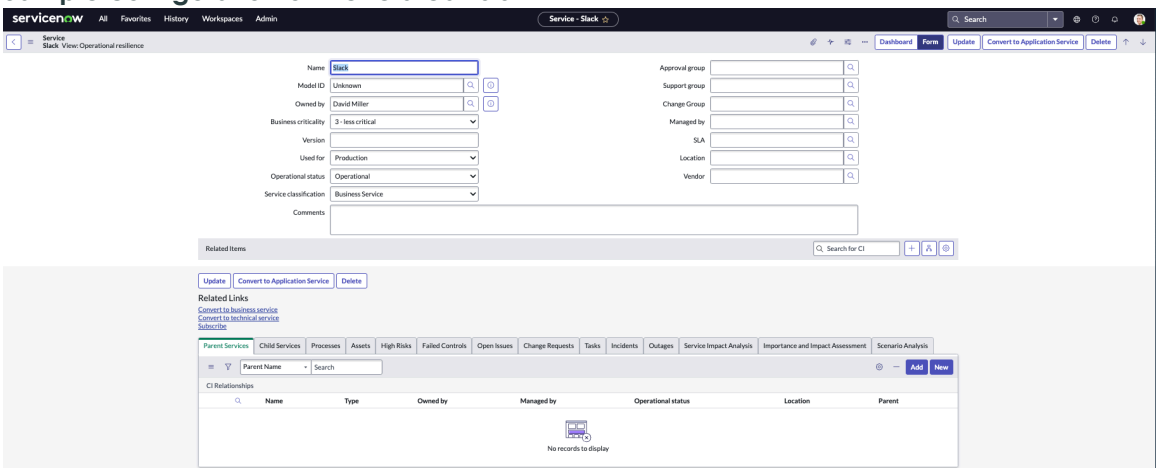
For more information on the Operational Resilience roles, see Roles installed with Operational Resilience.

## Related lists that are associated with a business service

When you add a business service, you can associate its dependencies as its related lists. Some examples are the parent services, child services, or processes on the Service form as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Sample configuration of the related lists




See the following table for more information on the related lists, their description, and the usage of the New and Add actions for each related list.

**Note:** Some of the actions in the following table require the itil role. Users with this role can access the CMDB tables.

### Related lists on the Service form

| Name | Description | New action | Add action |
|---|---|---|---|
| Parent Services | List of the services that are the parent service of the current service. | Service form where you can add a parent service. Creates a relationship between the new parent service and the current service.<br><br>Role: This action requires the itil role. | Opens a table view where you can select multiple services and add them as the parent services of the current service.<br><br>Role: This action requires the itil role. |
| Child Services | List of the services that are the child services of the current service. | Service form where you can add a child service. Creates a relationship between the new child service and the current service.<br><br>Role: This action requires the itil role. | Table view where you can select multiple services that you can add as the child services of the current service.<br><br>Role: This action requires the itil role. |
| Processes | List of the processes that are associated with the current service. | Not applicable | Table view where you can select multiple processes that you can add as the child services of the current service. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related lists on the Service form (continued)**

| Name | Description | New action | Add action |
|---|---|---|---|
| Assets | List of the assets that are associated with the current service. | Not applicable | Table view where you can select multiple assets (entities) that you can add as the downstream entities of the current service. |
| Issues | List of the overdue issues that are associated with the current service. | Issue form. When you submit the Issue form, the application creates a record in the Services with Issues table. | Not applicable |
| High Risks | List of the high-risk items or the risk assessments in the monitor state that are associated with the service. | Not applicable | Not applicable |
| Failed | List of the controls where the status of the control is non-compliant. | Not applicable | Not applicable |
| Change Requests | List of the open change requests that are associated with the current service. | Change Request form. When you submit the Change Request form, the application creates a record in the Services table. | Not applicable |
| Tasks | List of the open tasks that are associated with the current service. | List of the task tables, from where you can select the type of the task that you want to create. When you submit the form, the application creates a record in the Services with the Tasks table. | Not applicable |
| Incidents | List of the open incidents that are associated with the current service. | Incident form. When you submit the Incident form, it creates a record in the Services table. | Not applicable |
| Outages | List of the open outages that are associated with the current service. | Outage form. When you submit the form, the application creates a record in the Services table. | Not applicable |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related lists on the Service form (continued)**

| Name | Description | New action | Add action |
|---|---|---|---|
| Importance and Impact Assessment | List of the approved records of the Importance and Impact Assessments. | Not applicable | Not applicable |
| Scenario Analysis | List of the approved Scenario Analyses. | Not applicable | Not applicable |
| Business Continuity Plans | List of the approved Business Continuity Plans. | Not applicable | Not applicable |

**Note:** If the Business Continuity Management application is installed, its related list is displayed in Operational Resilience view.

For more information on the field values in the Service form, see Service form.

### Add a business service to the reporting dashboard

Add a business service and its related lists, such as the parent services, child services, processes, assets, and issues, in the Operational Resilience application so that you can view their operational resilience status on the reporting dashboard.

## Before you begin

Role required: sn_oper_res.manager

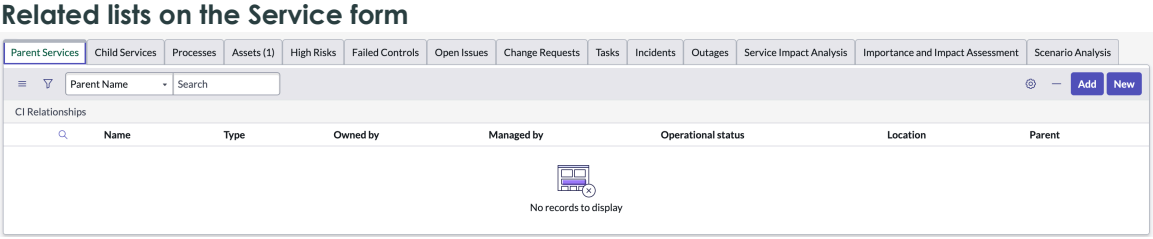
## About this task

When the *Compute Operational Resilience Compliance* scheduled job runs in the background daily, you can view the status reports of the business services on the Operational Resilience dashboard.

## Procedure

1. Navigate to **All** > **Operational Resilience** > **Services** > **Business Services**.
   A list of the available business services is displayed.
2. To mark a service as a critical service, or to add a service to Operational Resilience reporting, click **Add to OpRes reporting**.
   When you add a service to Operational Resilience, you can perform an analysis on the service. Any information that is reported on the service is displayed on the Operational Resilience dashboard. You can also view the reports of the related lists on the dashboard.
   When you add a service to Operational Resilience, the following informational message is displayed on the Service form: *1 service(s) is added to Operational Resilience reporting and dashboards.*.
3. Click a service to open its form and view its related lists.
   The related lists are displayed on the Service form as shown in the following example.

**Related lists on the Service form**

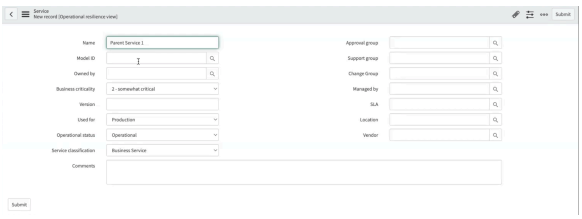
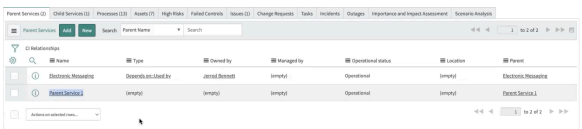
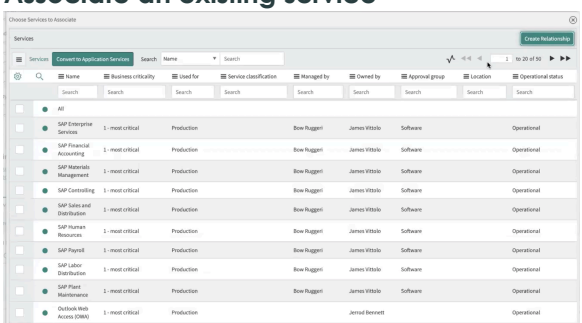



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

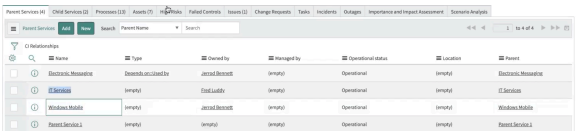
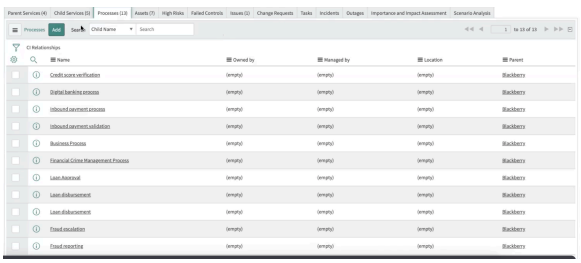
**Note:** When you add your business service to the Operational Resilience reporting dashboard, you can view its related lists and the Add or New actions for each related list on the Service form.

For a description of the field values on the Service form, see Service form.

4. Update the related lists by associating your business service with one or more parent services, child services, processes, and other configuration items as explained in the following table.

| Option | Description |
| --- | --- |
| Parent Services | Parent Services related list. Click **New** to create a service record for the service. The Service New record form is shown in the following example.<br>**Sample Service New record form**<br>  <br>After you click **Submit**, the parent service is added to the list as shown in the following example.<br>**Parent service in the related list**<br>  <br>Similarly, click **Add** in the Parent Services related list to associate an existing service with the service, select a service in the list view, and click **Create Relationship** as shown in the following example.<br>**Associate an existing service**<br>  <br>The service is added to the list as shown in the following example. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | **Parent Services related list**<br>  <br>If no entity is created with the newly created relationships (that is, associated services), the GRC application creates an entity. It also associates its upstream and downstream entities with this service. |
| Child Services | Child Services related list.<br>**Note:** You can follow the steps in the Parent Services section for the Child Services related list on the Service New record form. |
| Click Processes related list | Processes related list. The processes in the Business Process related list are shown in the following example.<br>**Processes related list**<br>  <br>Click **Add** and then click **Create Relationship** on the form to select multiple processes and relate them to the service directly. |
| Click Assets | Assets related list. Select one or more assets and click **Create Relationship** on the form to associate the assets with the service. |
| Click Issues | Issues related list. This action opens the GRC Issue form. Click **New** to create an issue that is related to the service and click **Submit**. The issue is displayed in the Issues related list.<br>**Note:** Only overdue issues are displayed on the Service form. You can create an issue, but when the scheduled job is executed, the issue is not displayed on the Service form or the reports. |
| Click Change Request. | Change Request related list. Click **New** to create a change request that is related to |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

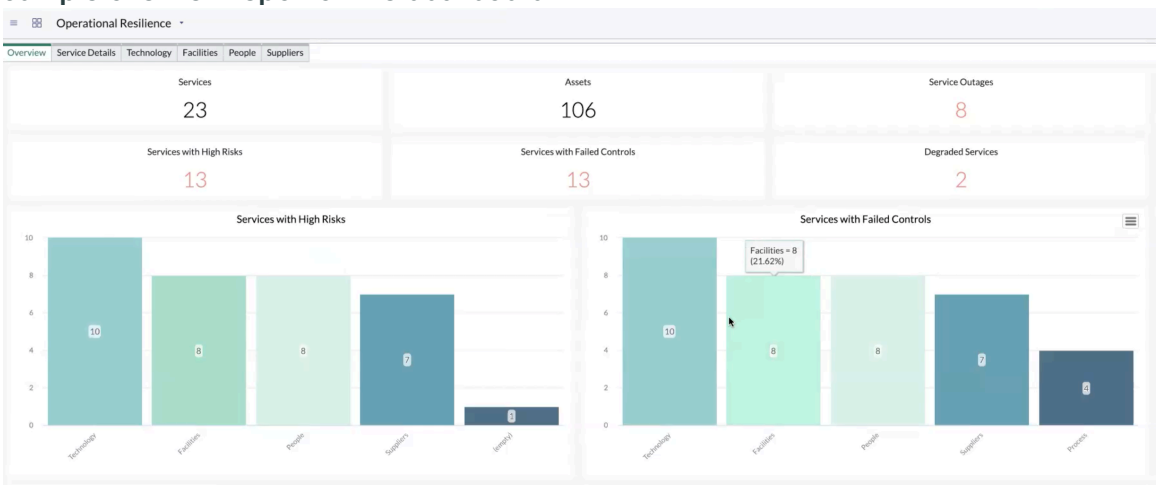
| Option | Description |
|---|---|
| | the service and click **Submit**. The change request is displayed in the Change Request related list. |
| Click Tasks | Tasks related list. Click **New** to create a task that is related to the service, enter the short description, and click **Submit**. The associated task is displayed in the Tasks related list. |
| Click Incidents | Incidents related list. Click **New** to create an incident that is related to the service, enter the caller name and a short description, and click **Submit**. The associated incident is displayed in the Incidents related list. |
| Click Outages | Outages related list. Click **New** and click **Submit** to create an outage that is related to the service. The associated outage is displayed in the Outages related list. |

**Note:** After you associate the configuration entities with the service as outlined in the table, you can view the reports on the Operational Resilience dashboard.

**Result**

After you set up the parent services, child services, and other related lists for a business service, the *Compute Operational Resilience Compliance* scheduled job collects the associated data from the integrated applications. You can view the reports of the associated configuration items, such as the services, assets, or processes, on the dashboard as shown in the following example.

**Sample overview report on the dashboard**




### Service form

Use the Service form to set up a business service and configure its related lists.

## Service form

For a description of the field values, see the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Service form

| Field | Description |
|---|---|
| Name | Name of the business service. |
| Model ID | Model ID for the business service. |
| Owned by | Owner of the business service. |
| Business criticality | Criticality of the business service. The available options are as follows:<br>• 1—most critical<br>• 2—somewhat critical<br>• 3—less critical<br>• 4—not critical |
| Version | Version of the business service. |
| Used for | Category that the service is used for. For example, Staging. The available options are as follows:<br>• Production<br>• Staging<br>• QA<br>• Test<br>• Development<br>• Demonstration<br>• Training<br>• Disaster recovery |
| Operational status | Operational status of the business service. The available options are as follows:<br>• Operational<br>• Non-Operational<br>• Repair in Progress<br>• Dr Standby<br>• Ready<br>• Retired<br>• Pipeline<br>• Catalog |
| Service classification | Classification of the service. The available options are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Service form (continued)

| Field | Description |
|---|---|
| | • Business Service<br>• Technical Service<br>• Application Service |
| Approval group | Approval group that is responsible for the approval of the business service. For example, Application Development or Application Security group. |
| Support group | Support group that is responsible for supporting the business service, such as Capacity Management. |
| Change group | Change group that is responsible for updating the business service. |
| Managed by | Manager that is responsible for managing the business service. |
| Location | Location of the business service. |
| Vendor | Vendor that is responsible for the business service. |
| Comments | Additional comments that are related to the business service. |
| Related items | Dependencies that are associated with the business service. |

## Related lists

### Related lists that are associated with the service

| Related list | Description |
|---|---|
| Parent Services | Configuration Item (CI) relationship type for the parent service.<br><br>When you add a parent service to a business service, an entity is automatically created for the added parent service. The new service entity is added to the upstream entity of the business service's entity. |
| Child Services | Configuration Item (CI) relationship type for the child service.<br><br>When you add a child service to a business service, an entity is automatically created for the added child service. The new service |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related lists that are associated with the service (continued)**

| Related list | Description |
|---|---|
| | entity is added to the downstream entity of the business service's entity. |
| Processes | Supporting service processes. You can add a process to the service.<br><br>When you add a child process to a business service, an entity is created for the child process. The new process entity is added to the downstream entity of the business service's entity. |
| Assets | Assets that are associated with the business service. You can add an asset to the service. |
| High Risks | Details of the risks that are associated with the current service. |
| Failed Controls | Details of the failed controls that are associated with the current service. |
| Open issues | Open issues that are associated with the current service. You can create an issue for the service. |
| Change Requests | Change requests that are associated with the current service. You can create a change request for the service. |
| Tasks | Tasks that are associated with the current service. |
| Incidents | Incidents that are associated with the current service. You can create an incident for the service. |
| Outages | Outages that are associated with the current service. You can create an outage for the service. |
| Service Impact Analysis | Service impact analysis that is associated with the current service. You can create a service impact analysis for the service. |
| Importance and Impact Assessment | Importance and impact assessment that is associated with the service.<br><br>The importance of a business service is determined by a survey type analysis. The impact tolerance of a business service specifies how long a service can be operational without causing any disruptions. For example, the sample factors considered are the number of customers, revenue, impact on the brand, and other strategic impacts for a financial organization. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related lists that are associated with the service (continued)**

| Related list | Description |
|---|---|
| | After the analysis is completed, the value is stored in the CMDB so that this information is used by other users. |
| Scenario Analysis | Scenario analysis that is associated with the business service. |

## Analyzing the importance and impact tolerance of the business services

By analyzing the importance and the impact tolerance of your business services, you can measure how disruptions might impact your services. You can use an assessment questionnaire template in the Operational Resilience application to measure the importance and the impact tolerance of your business services.

## Importance and impact tolerance of a business service

A business service's importance is determined by such factors as the number of customers that use the service, the revenue that the service generates, and its impact on your company's brand. By measuring the impact tolerance of a business service, you can see how long a service can be non-operational without causing some kind of loss to the business and its customers.

You can use the Operational Resilience application to perform an assessment that measures the importance and the impact tolerance of your business services.

## Workflow and assessment states

If you have the sn_oper_res.manager role, you can create and maintain a pre-defined assessment questionnaire template. By selecting one or more business services that you want to analyze, you can then use an assessment template to calculate the importance and the impact tolerance of these services.

The owner and assessor of the assessment typically perform the following tasks:

- The owner of the assessment selects the business services and submits the Importance and Impact Tolerance assessment for one or more business services in the Operational Resilience application. This action creates an assessment instance that contains the questions from the questionnaire template.
- The assessor of the assessment receives an email notification with a link to the assessment.
- The assessor clicks the link to the assessment and responds to the questionnaire. Based on the assessor's responses to the questionnaire, an assessment of the importance rating and the tolerable duration for one or more of your business services is generated.
- The owner requests an approval after the assessment is completed.
- The owner verifies the responses to the questions. The owner's responses may override the importance and impact tolerance rating of the assessment.
- The approver approves the assessment for the business service.
- The owner closes the assessment after it has been approved.

When you perform the assessment tasks, the assessment is updated through different states in the Operational Resilience application as shown in the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### States for Importance and Impact Tolerance assessment

| State | Description |
|---|---|
| Draft | The owner of the assessment selects the questionnaire template and initiates an assessment to assess one or more business services. The assessment is created in the **Draft** state by default.<br><br>The owner adds the business services to assess from the Services related list and submits the assessment. |
| Pending Response | When the owner submits the assessment, it creates an assessment instance for the assessor. The instance has questions from the questionnaire template.<br><br>The state of the assessment is then automatically updated to the **Pending Response** state. The assessor receives an email notification with a link to the assessment. |
| Response Received | When the assessor responds to the questionnaire in the assessment, the state of the assessment is automatically updated to **Response Received**.<br><br>An importance rating and the duration of the impact tolerance are automatically generated based on the questionnaire responses. The owner of the assessment can request an approval. |
| Pending Approval | The approver verifies the responses to the questions and may override the importance and impact tolerance rating of the assessment. The state of the assessment is then automatically updated to **Pending Approval**. |
| Canceled | The owner can cancel an invalid or incorrect assessment. Clicking **Cancel** moves the state of the assessment to the **Cancelled** state. The owner can cancel the Importance and Impact Tolerance Assessment in **Pending Response** or **Pending Approval** state. |
| Approved | When an approver approves the assessment for the selected business service, the state of the assessment is automatically updated to **Approved**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States for Importance and Impact Tolerance assessment (continued)**

| State | Description |
|---|---|
| Closed | After an assessment is approved, the owner can close the assessment. An assessment can be closed only when it is in an **Approved** state. By clicking **Close**, you move the state of the assessment to the **Closed** state. |

**Note:** If you have the sn_oper_res.admin role, you can delete the Importance and Impact Tolerance assessment in any state.

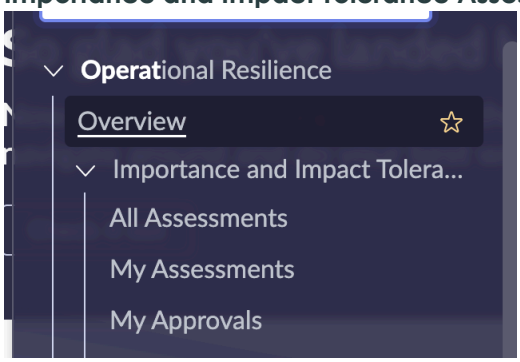
For more information on the Operational Resilience roles, see Roles installed with Operational Resilience.

Email notifications: When a user with the sn_oper_res.manager role assigns the assessment, an email notification is automatically sent out to inform the assessor and the approver about the assignment.

## Viewing the Assessments

If you have the sn_oper_res.manager role, you can view the assessments by navigating to the **All** > **Operational Resilience** > **Importance and Impact Tolerance Assessment** module in the application UI as shown in the following example.

**Importance and Impact Tolerance Assessment module**




- All Assessments: If you have the sn_oper_res.manager role, you can view all the related assessments under All Assessments.
- My Assessments: If you have the sn_oper_res.user role, you can view the assigned assessments under My Assessments.
- My approvals: If you have the sn_oper_res.user role, you can view the assigned approvals under My Approvals.

## Setting up the assessment ratings

If you have the sn_oper_res.admin role, you can set up the assessment ratings by updating the criticality and order of the assessment rating in the Important choices module. For more information on setting up the assessment rating, see Update the assessment rating in the Important choices module.

### Create an assessment for your services

Create an assessment in the Operational Resilience application to measure the importance and impact tolerance of your business services.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin

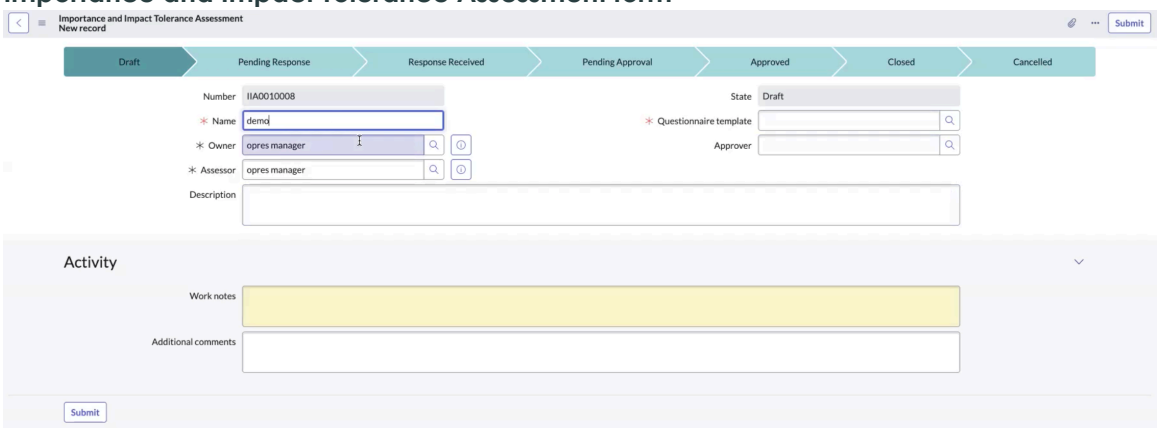
Role required: sn_oper_res.user, sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience** > **Importance and Impact Tolerance Assessments** > **All Assessments**.
2. Click **New**.

   This action creates an assessment form so that you can measure the importance and impact tolerance of your business service.

**Importance and Impact Tolerance Assessment form**




3. In the **Name** field, enter the name of the assessment.
4. Verify that the name of the logged-in user is displayed in the **Owner** field and the **Assessor** field of the assessment.

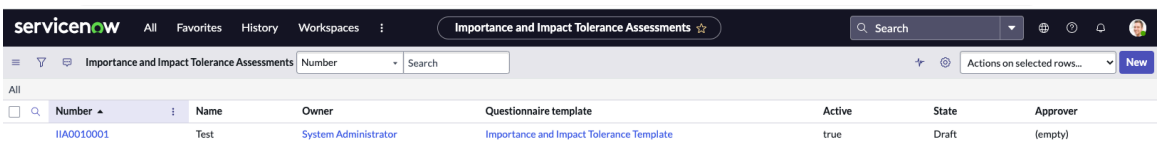
   **Note:** The user who submits an assessment is its assigned owner and assessor by default.

5. In the **Questionnaire template** field, select the Importance and Impact Tolerance Template from the available options.
6. In the **Approver** field, select an approver for the assessment.
   For a description of the field values on the Importance and Impact Tolerance Assessment form, see Importance and Impact Tolerance Assessment form.

   **Note:** The owner of the assessment can't be its approver.

7. Click **Submit**.
   A new assessment is created in the **Draft** state. It is displayed in the Importance and Impact Tolerance Assessments list as shown in the following example.

**New assessment**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Result
The state of the assessment moves to the **Draft** state and a questionnaire is sent to the assessor about the business services.

#### Importance and Impact Tolerance Assessment form

Use the Importance and Impact Tolerance Assessment form to create an Importance and Impact Tolerance assessment for your business services.

## Importance and Impact Tolerance Assessment form
For a description of the field values, see the following table.

**Importance and Impact Tolerance Assessment form**

| Field | Description |
|---|---|
| Name | Name of the assessment. |
| Description | Description of the assessment. |
| Number | Number for the assessment. This field is auto-filled. |
| Owner | Owner of the assessment. This field is auto-filled. |
| Assessor | Assessor of the assessment. This field is auto-filled. |
| State | State of the assessment. This field is auto-filled. |
| Questionnaire template | Default questionnaire template to be filled by the customer. |
| Approver | Approver of the assessment. |
| Activity journal | Work notes and additional comments that are associated with the assessment. |
| Related lists (Displayed on the form after a service is added) | |
| Services | Business services that are associated with the assessment.<br>**Note:** You can add the services of only a business service type to an assessment. |
| Assessment instances | Assessment instance for the assessor that has the questions from the questionnaire template. |
| Approvers | Approvers of the assessment. |

#### Submit an Importance and Impact Tolerance assessment

Submit an assessment in the Operational Resilience application to measure the importance and the impact tolerance of your business services.

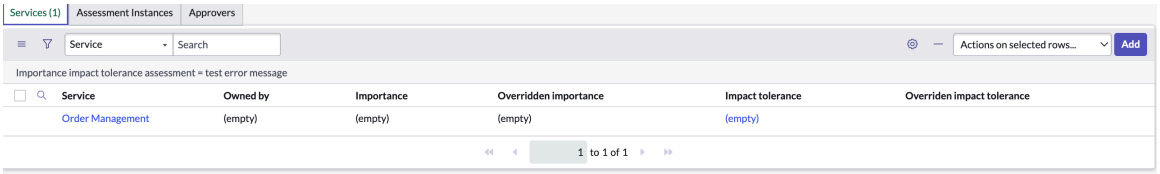
### Before you begin
Role required: sn_oper_res.user, sn_oper_res.manager

### Procedure

1. In the Importance and Impact Tolerance Assessments list, click an assessment that is in the **Draft** state.
   The related lists that are associated with the assessment are displayed as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Related lists for the assessment

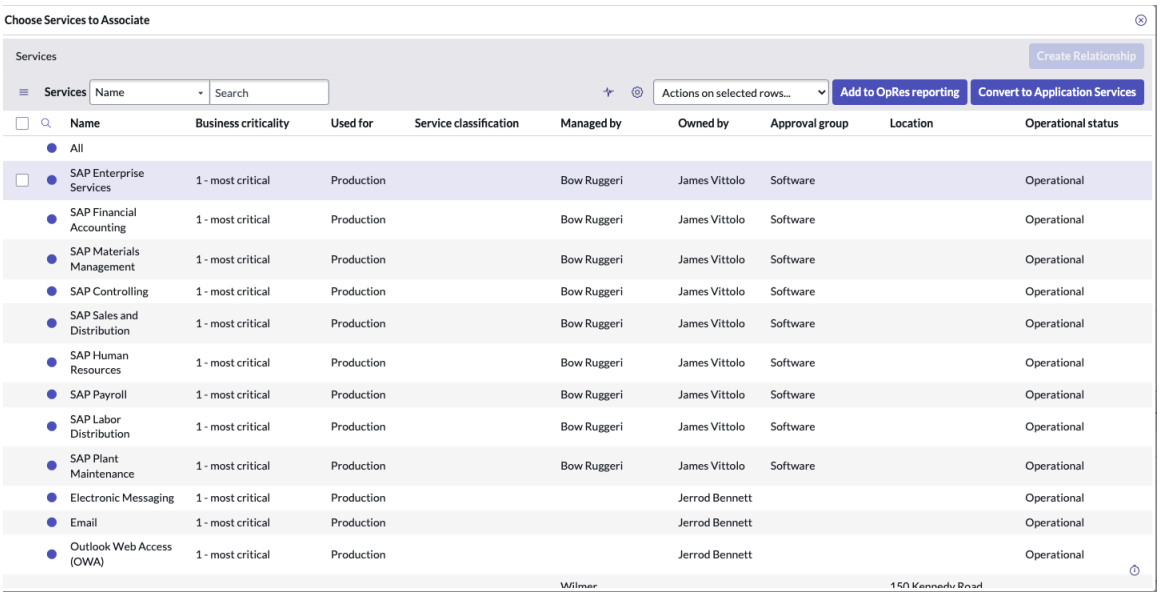



2. In the Services related list, select a service that you want to associate with the assessment and click **Create Relationship**.

   **Note:** Before you submit the assessment, you must associate at least one service with it.

   The Services list view is shown in the following example.

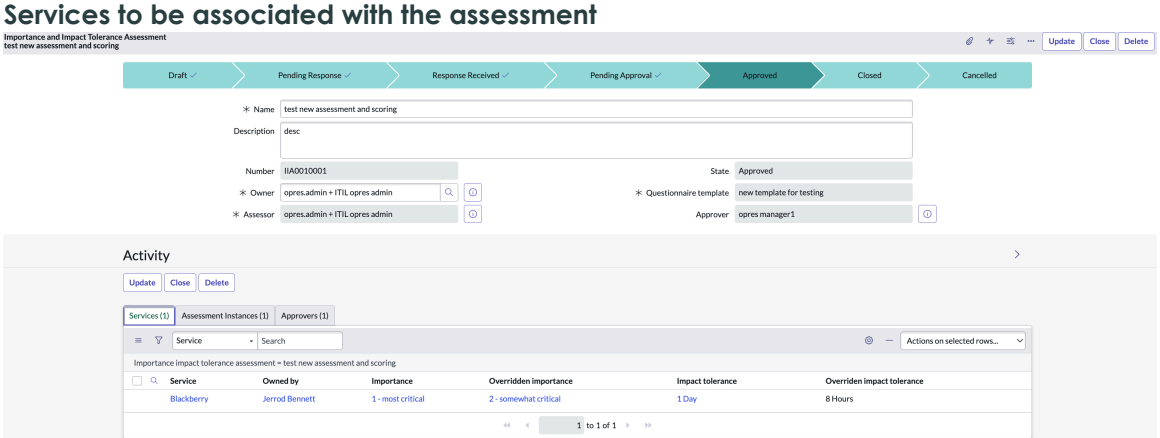
### Services list




   The service that is associated with your assessment is displayed in the Services related list.

3. Click the **Assessment Instances** related list and verify the assessment instance. Associating a service with your assessment displays an assessment instance in the related list as shown in the following example.

### Services to be associated with the assessment




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Click the **Approvers** related list and verify the approvers of the assessment.
5. Click **Submit**.

### Result
The state of the assessment changes to **Pending Response** and the assessor receives an email notification with a link to the assessment.

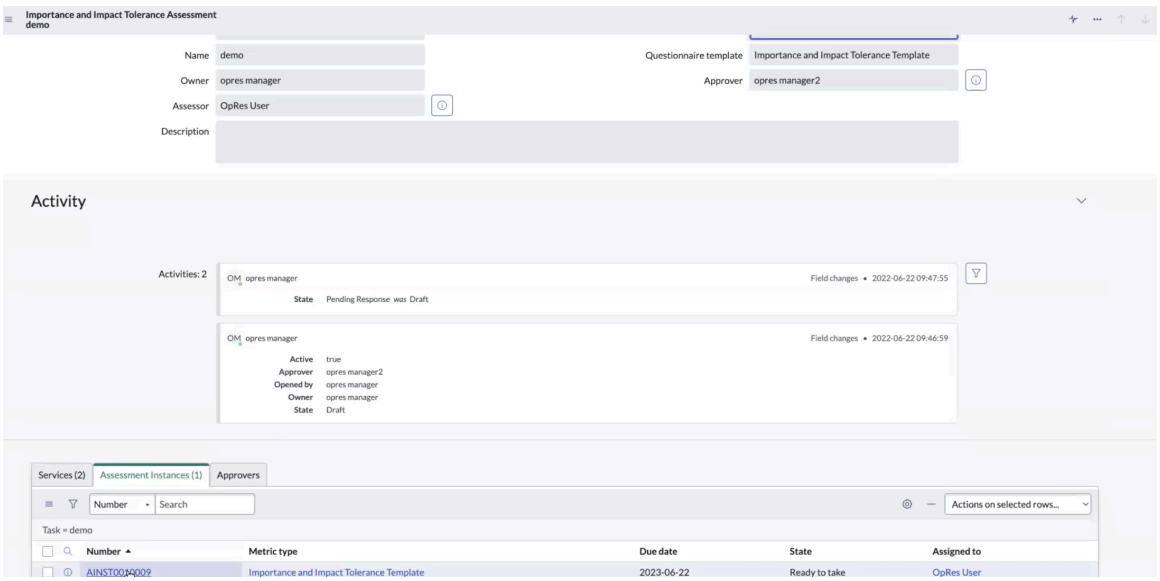
## Respond to the Importance and Impact Tolerance assessment

Log in as an assessor of the assessment in the Operational Resilience application and respond to the questions to measure the importance and impact tolerance of your business services.

### Before you begin
Role required: sn_oper_res.user

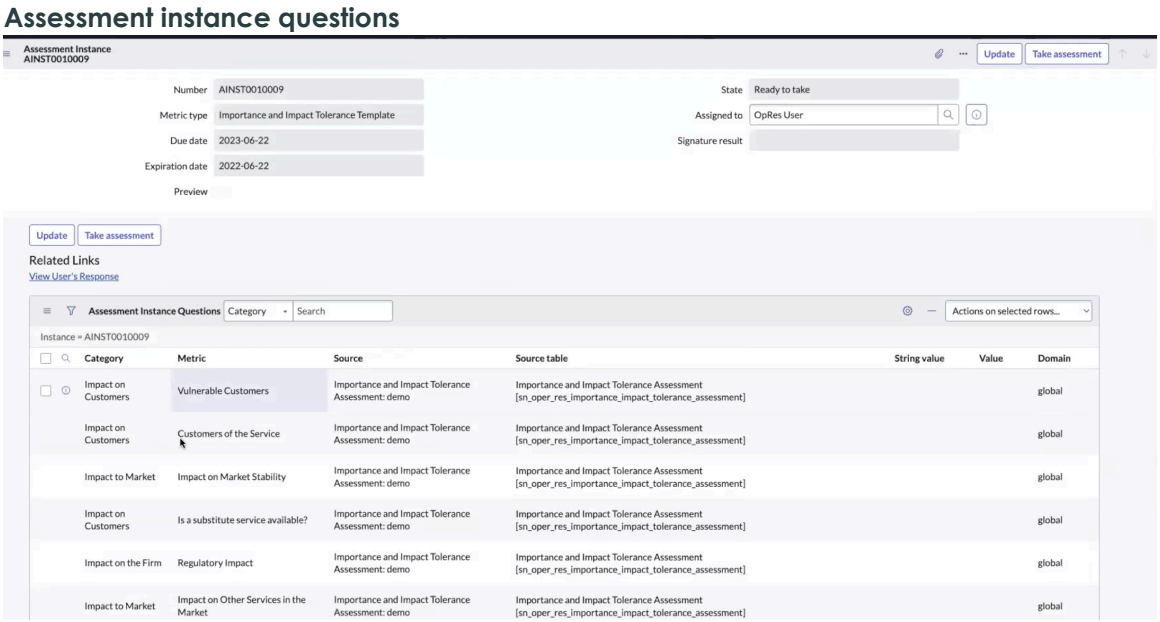
### Procedure
1. Navigate to **All** > **Operational Resilience** > **Importance and Impact Tolerance Assessments** > **My Assessments**.
   As an assessor of the assessment, you can access the assessment in the Assessment Instances list as shown in the following example.

**Assessment instances list**




2. Click the assessment instance that is listed in the Assessment Instance related list.
   Clicking the assessment instance displays the questionnaire as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. Click **Take assessment**.
   The assessment questions are populated in the template as shown in the following example.




4. Respond to the questions and click **Submit**.
   When you submit the assessment, the following informational message is displayed on the screen: *You have completed this risk assessment*. As the assessment owner, you can track its progress in the Assessments related list of the form.

## Result

The state of the assessment changes to **Response Received**.

### Override the rating of your assessment

Override any discrepancies that you see in the importance and the impact tolerance rating of the assessment about your services while you're verifying the responses in the Operational

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Resilience application. This way, you can make sure that an accurate rating is assigned to your business services.

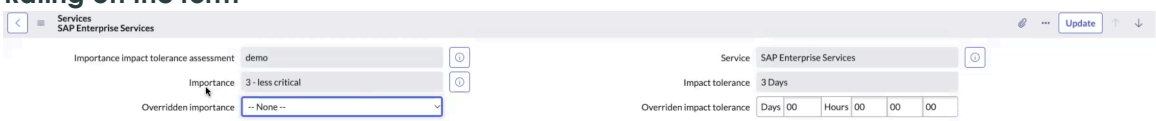
### Before you begin

Role required: sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience** > **Importance and Impact Tolerance Assessments** > **All Assessments** > **Assessment** > **Assessment Instances**.
2. Click the assessment and navigate to its Services list.
3. Open the Service record.
4. View the importance and impact tolerance rating for your service.
   Based on the score of the assessment, the rating for the importance and impact tolerance is auto-filled in for your service as shown in the following example.

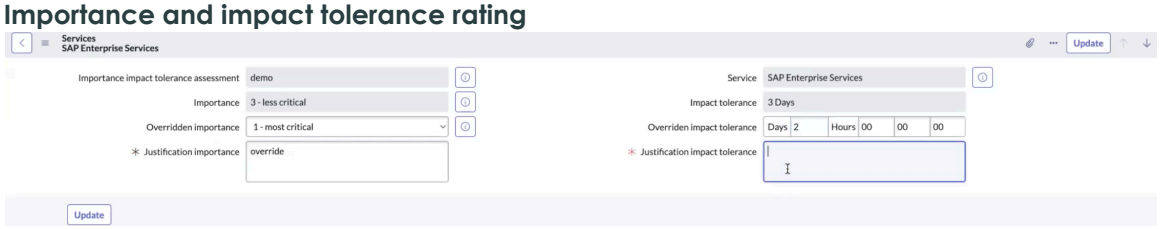
**Rating on the form**




5. Override the importance of the service by updating the importance value in **Overridden Importance** to one of the following options:
   - **None**
   - **Most critical**
   - **Somewhat critical**
   - **Less critical**
   - **Not critical**

   For information on the default importance rating scales, see Set up the Importance and Impact Tolerance Rating Scale.
6. Update the **Justification importance** field with the reason for overriding the importance.
7. To override the impact tolerance rating of the service, update the rating in the **Overridden impact tolerance** field.
   Based on your assessment, you can override the importance and impact tolerance rating of the service as shown in the following example.

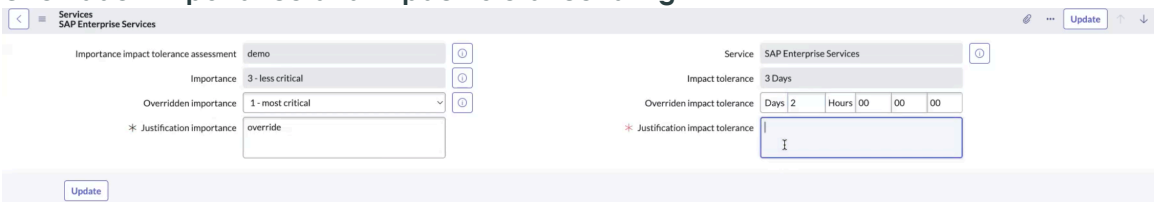
**Importance and impact tolerance rating**




8. Update the **Justification impact tolerance** field with the reason for overriding the impact tolerance.
9. Click **Update**.
   The importance and impact tolerance of the associated service is displayed for each service in the Services record. View the rating of your service in the Services related list as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Overridden importance and impact tolerance rating




**Note:** You can override the importance and impact tolerance rating of your service only when the assessment is in the **Response Received** and **Pending Approval** state.

**Result**
The state of the assessment changes to the **Pending Approval** state.

### Approve and close the assessment

Approve the Importance and Impact Tolerance assessment in the Operational Resilience application for your business services so that you can notify the owner and close the assessment.

**Before you begin**
Role required: sn_oper_res.manager

**About this task**
After the assessment is approved, a notification is automatically sent to the owner of the service that the assessment is approved. The owner can then close the assessment.

**Procedure**

1. Navigate to **All** > **Operational Resilience** > **Importance and Impact Tolerance Assessments** > **My Approvals**.
2. In your instance, log in as the approver of the assessment, view your open assessment, and click **Approve**.
   After you approve the assessment, a notification is automatically sent to the owner of the service that the assessment is approved. The state of the assessment changes to the **Approved** state. After the assessment is complete, the Services record form is in the read-only state as shown in the following example.

**Read-only state for the rating**




3. To close the assessment, click **Close**.

**Result**
The state of the assessment changes to **Closed**.

## Performing a scenario analysis of the business services

You can define the risks that might impact your business with a scenario analysis of your business services in the Operational Resilience application. By adding participants, such as your users with the sn_oper_res.manager or sn_oper_res.user roles from the associated business functions to your scenario analysis, you can collect their inputs, calculate the possible disruptions, and determine if a service was breached.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Overview of a scenario analysis

Scenarios represent the business-specific risks that are used to test how events can impact your organization. If you have a scenario analysis, you can determine the operational resilience of your business services. For example, if you have the sn_oper_res.manager role, you can use the Scenario Analysis form in the application to select the business services, the participants that are associated with the business functions, and the associated scenario events to analyze.

After you analyze all the scenario events, you verify the status of the services and calculate the duration of the disruption. You can also collate the gaps, recommendations, and observations from the participants to complete the analysis. Next, you request that an approver approves the scenario analysis. After it's approved, you close it and see its status in the dashboard.

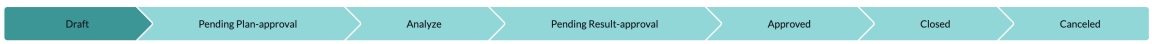
## Tasks to set up a scenario analysis and workflow states

If you have the sn_oper_res.manager role, you can set up a scenario analysis for your business services. As a scenario analysis owner, you can do the following tasks:

- Create a scenario that helps you to determine the risks that are applicable to your business.
- Add the services, participants, scenario events, and approvers to your scenario.
- Associate one or more events with a scenario.
- Perform a scenario analysis and collect the observations, gaps, and recommendations from the participants about the scenario analysis events. The participants of a scenario analysis are the users with the sn_oper_res.manager or sn_oper_res.user roles from the associated business functions, such as Finance or HR departments. These participants can add their work notes that are related to a scenario.
- Calculate the disruption to your services and determine if any service was breached.
- Send your analysis for a review to the approver of the scenario and request an approval.
- Close the approved scenario analysis.

When you set up a scenario analysis in the Operational Resilience application, it is associated with the states that are shown in the following table.

**States that are associated with a scenario analysis**




**States that are associated with a scenario analysis**

| State | Description |
|---|---|
| Draft | First state of the scenario analysis. If you have the sn_oper_res.manager role, you can initiate a scenario analysis, provide the name and description of the analysis, and analyze one or more scenarios and associated events. The sn_oper_res.manager (the logged-in user) is automatically displayed as the owner of the scenario in the Owner field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States that are associated with a scenario analysis (continued)**

| State | Description |
|---|---|
| | If you're an analysis owner, you can add your business services, participants, and scenarios to the analysis and assign a plan-approver and result-approver to it.<br><br>When you submit the scenario analysis, a notification is sent to the plan-approver. The state of the scenario analysis is updated to the **Pending Plan-approval** state.<br><br>**Note:** You must associate at least one service before moving the scenario analysis to the **Pending Plan-approval** state. |
| Pending Plan-approval | Second state of the scenario analysis. As a pending plan-approver, you must review the scope of the analysis in this state. You can check the setup of the services, participants, associated scenario events, and approvers and then approve the analysis. When you approve the analysis, the state of the scenario analysis is updated to the **Analyze** state. |
| Analyze | Third state of the scenario analysis. In this state, the participants of the scenario analysis can add work notes on the Scenario Analysis form and work on events that are based on their responsibility.<br><br>If you're the analysis owner, you must collect the feedback from the participants and submit their observations, gaps, and recommendations for each associated event on the form. When you submit this information, the state of the scenario analysis is updated to the **Pending Result-approval** state. |
| Pending Result-approval | Fourth state of the scenario analysis. In this state, the summary details of the scenario analysis are auto-filled in the application on the Scenario Analysis form.<br><br>If you're the scenario analysis owner, you can verify the details, check if any of your services are breached, and request the result-approval for the analysis.<br><br>If you're the result-approver, you can review the analysis scope in this state, ensure that |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States that are associated with a scenario analysis (continued)**

| State | Description |
|---|---|
| | it is a valid analysis for the selected business services, and approve or reject the analysis.<br><br>When you approve the analysis, the state of the scenario analysis is updated to the **Approved** state. |
| Approved | Fifth state of the scenario analysis. In this state, an email notification is also sent to the approver for reference.<br><br>When the state of the scenario analysis is in the **Approved** state, you can close it. |
| Closed | Final state of the scenario analysis. As the analysis owner, when you close the analysis, its state is updated to **Closed**. |

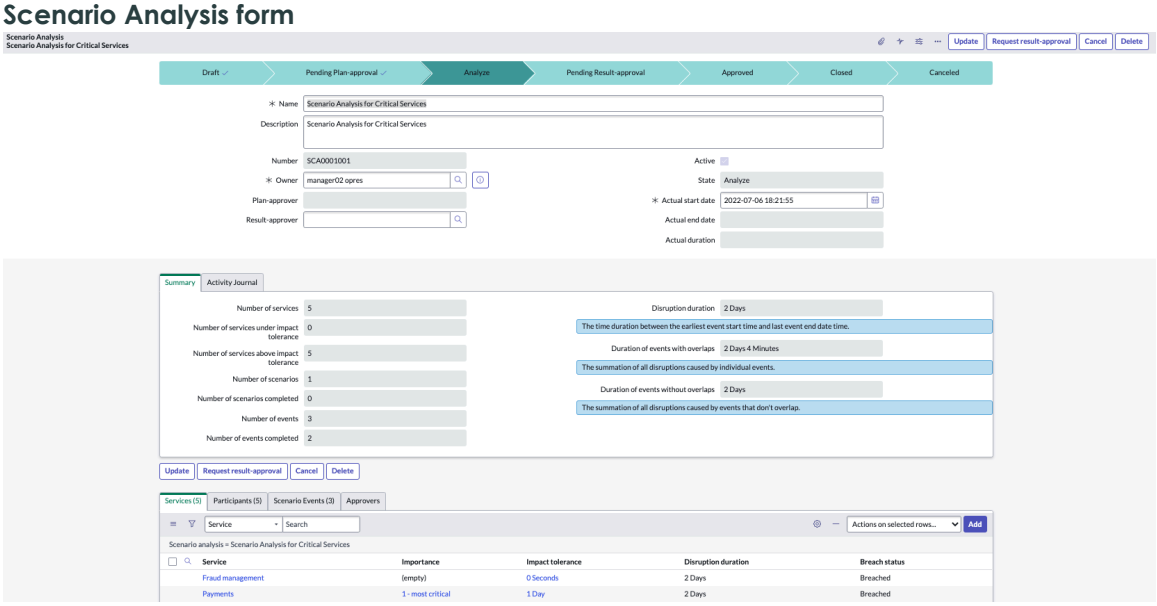
For more information on the Operational Resilience roles, see Roles installed with Operational Resilience.

## Summary of your scenario analysis

While you are doing the scenario analysis, you can verify the status of your business services in the Summary panel of the Scenario Analysis form in the Operational Resilience application.

A typical Scenario Analysis form is shown in the following example.

**Scenario Analysis form**




The Summary panel provides information about your business services, associated scenarios, disruptions, and events. For a description of the field values, see the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

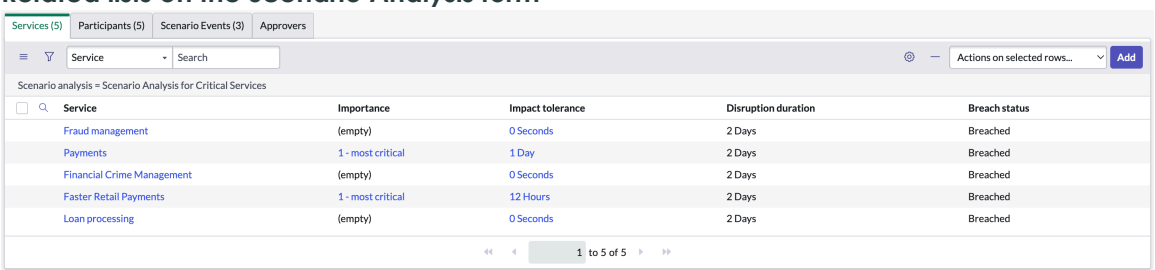
### Summary of your services, scenarios, disruptions, and events

| Field | Description |
|---|---|
| Number of services | Number of services that are associated with the scenario analysis. |
| Number of services under impact tolerance | Number of services that are associated with the scenario analysis and that are under impact tolerance. |
| Number of services above impact tolerance | Number of services that are associated with the scenario analysis and that are above impact tolerance. |
| Number of scenarios | Number of scenarios that are associated with the analysis. |
| Number of scenarios completed | Number of completed scenarios that are associated with the analysis. |
| Number of events | Number of events that are associated with the analysis. |
| Number of events completed | Number of completed events that are associated with the analysis. |
| Disruption duration | Time duration between the end time of the last event and the start time of the first event. It is displayed in the number of days. |
| Duration of events with overlaps | Summary of all event durations including the overlapping events and pauses. It is displayed in the number of days and minutes. |
| Duration of events without overlaps | Summary of all event durations without the overlapping events and pauses. It is displayed in the number of days and minutes. |

## Related lists on the Scenario Analysis form

When you create a scenario analysis, the related lists are displayed on the form as shown in the following example.

### Related lists on the Scenario Analysis form




You can configure the related lists on the Scenario Analysis form by using the New and Add actions as shown in the example. See the following table for the names, description, and actions that are associated with the related lists on the Scenario Analysis form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related lists on the Scenario Analysis form**

| Name | Description | New action | Add action |
|---|---|---|---|
| Services | List of the services | Not applicable | Table view where you can select multiple services that you can add to the current scenario analysis.<br><br>Role: This action requires the sn_oper_res.admin role or you should be the owner of the scenario analysis to add a service. |
| Participants | List of the participants of the current scenario analysis. | Action to create a participants record. Role: You must have the sn_oper_res.user role to perform this action. | Not applicable |
| Scenario events | List of the scenario events that are associated with the current scenario analysis. | Not applicable | Table view where you can select multiple scenario events that you can add to the current scenario analysis.<br><br>Role: This action requires the sn_oper_res.admin role or you should be the owner of the scenario analysis to add a scenario event. |
| Approvers | List of the approvers that are associated with the current scenario analysis. | Not applicable | Not applicable |

## Setting up your services with the sn_oper_res.critical_services property

You can analyze the importance and the impact tolerance of your business services by using the assessment questionnaire template in the Operational Resilience application. For information on analyzing the importance and impact tolerance of your business services, see Analyzing the importance and impact tolerance of the business services.

As the scenario analysis owner, you can select the services that you have already assessed with calculated importance and impact tolerance. You have to ensure that the selected services meet the entity filter condition that is defined in the entity type whose sys_id is

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

defined in the *sn_oper_res.critical_services* property. For information about this property, see Properties installed with Operational Resilience.

### Add a participant to your scenario analysis

Add a participant to your scenario analysis in the Operational Resilience application so that you can collate their observations about the scenario. You can add various participants who belong to the business functions that are associated with your services. You can use that information as a reference to perform the scenario analysis.

## Before you begin

Role required: sn_oper_res.admin

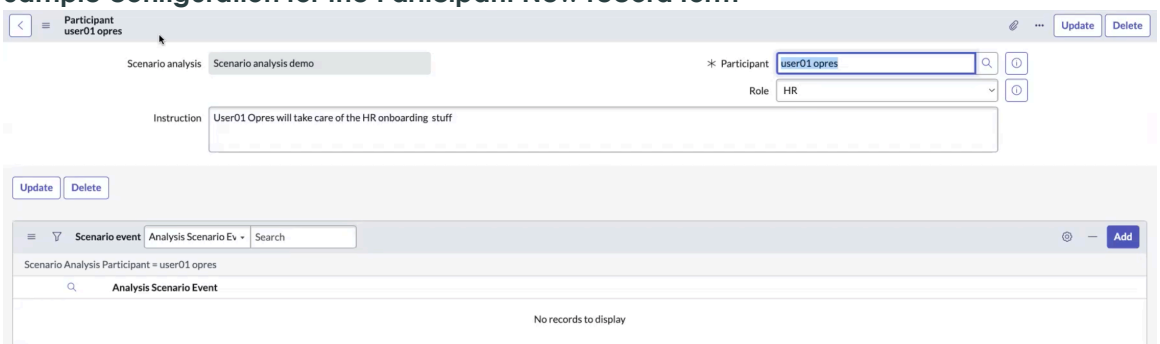
## About this task

A participant can add notes, observations, and recommendations about the scenario on the event form. The owner of the scenario analysis collects these inputs about the scenario event from the participants in the scenario event information record.

## Procedure

1. Navigate to **All** > **Operational Resilience** > **All Scenario Analyses** > **All Scenario Analyses**.
2. Open a scenario that you want to add a participant to.
3. In the Participants related list, click **New**.
   See the sample configuration for a participant in the following example.

**Sample configuration for the Participant New record form**




   In the Participant New record form, the name of the scenario analysis is auto-filled.
4. In the **Instruction** field, add the instructions for your participant.
5. In the **Participant** field, select a participant from the available options.
6. In the **Role** field, assign a role to the participant from the available options.
7. Click **Update**.
   You have added a participant to the scenario analysis. The participants related list is automatically updated in the Scenario Analysis record.

### Participant New record form

Use the Participant New record form to add a participant to your scenario analysis.

## Participant New record form

For a description of the field values, see the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Participant New record form

| Field | Description |
|---|---|
| Scenario analysis | Unique name for the scenario analysis. This field is auto-filled. |
| Instruction | Instructions for your participant. |
| Participant | Participant that you associate with the scenario analysis. |
| Role | Role that you assign to a participant. The available options are as follows:<br>• HR<br>• Legal<br>• Finance<br>• Technology<br>• People<br>• Data<br>• Security<br>• Supplier Tier1<br>• Supplier Tier2<br>• Supplier Tier3<br>• Procurement<br>• Facilities<br>• Mid-Level<br>• Managers<br>• Senior Managers<br>• Contractors<br>• Full Time Employees |

### Perform a scenario analysis of your services

Perform a scenario analysis of your services in the Operational Resilience application so that you can understand what the impact of the associated events and possible disruptions might be to your organization. After analyzing the scenario events, you can determine if any of your services are breached.

#### Before you begin

Role required: sn_oper_res.manager

#### About this task

If you have the sn_oper_res.manager role, you can create and publish an analysis. Only the owner of the scenario analysis and the user with the sn_oper_res.admin role can edit the analysis. After you review the analysis, you can request an approval. When the analysis is in the **Approved** state, you can close it.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **Operational Resilience** > **All Scenario Analyses** and click **New**.
2. In the **Name** field, enter the name of the scenario analysis record.

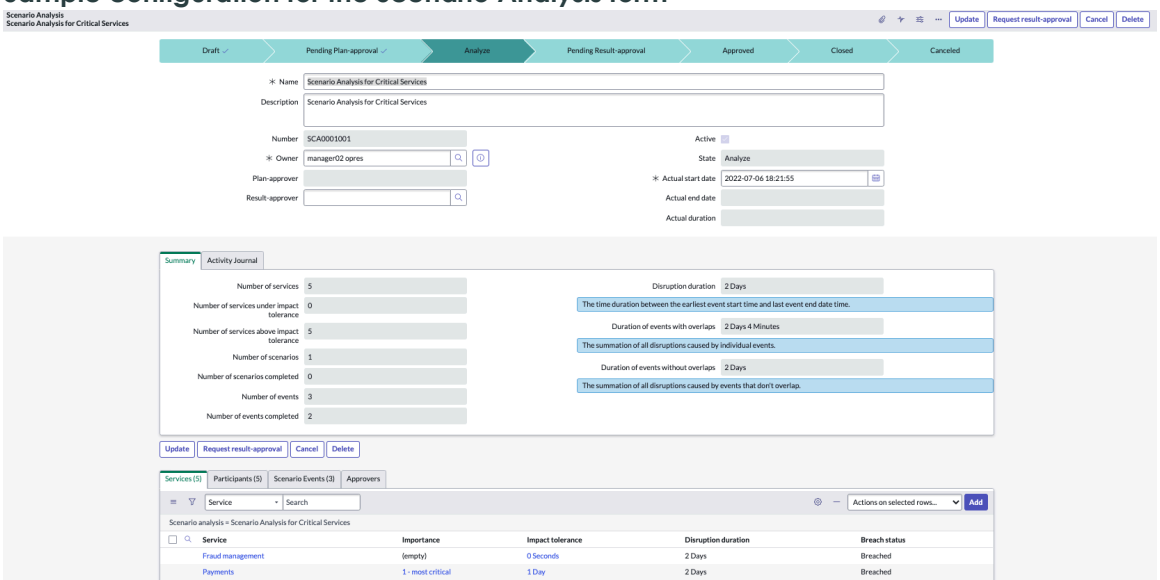
   The logged-in user is set as the owner of the scenario analysis record and the state of the scenario analysis is updated to **Draft** by default. The Summary panel displays the detailed information on the services, disruption, and events that are associated with the scenario analysis.

3. In the **Plan-approver** field, select the plan-approver for the scenario analysis:
   - Click **New** to add a new user record for the plan-approver by using the lookup list.
   - Click **Submit**.

   For the descriptions of the field values on the User New record form, see Scenario Analysis form.

   See the sample configuration for the Scenario Analysis form as shown in the following example.

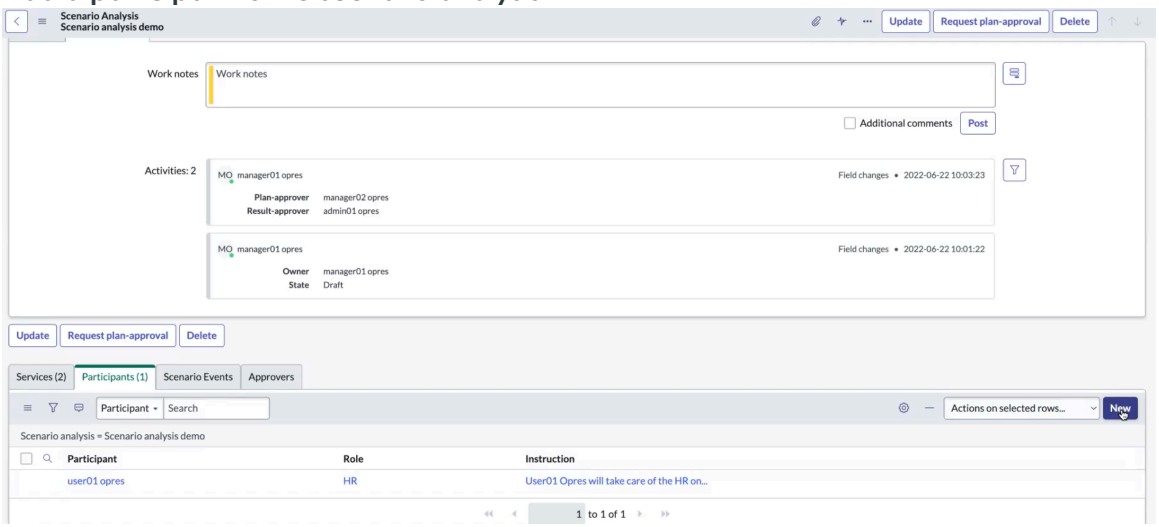
**Sample configuration for the Scenario Analysis form**




4. In the Services related list, associate at least one service with the scenario.
5. Click **Begin analysis**.
   If you begin analysis without associating at least one service with the scenario, the following informational message is displayed: *`Associate at least one service to begin the analysis.`* In the Summary panel, the number of services, the number of services under impact tolerance, and the number of services over impact tolerance are updated. For a description of the field values on the form, see Scenario Analysis form.
6. In the **Plan-approver** field, assign the plan approver for the scenario analysis.
7. In the **Plan-approver** field, assign the result approver for the scenario analysis.
8. In the **Actual start date** field, enter the actual start date for the analysis.
9. Add a participant to the scenario analysis.
   You can add a participant to the scenario analysis as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Add a participant to the scenario analysis



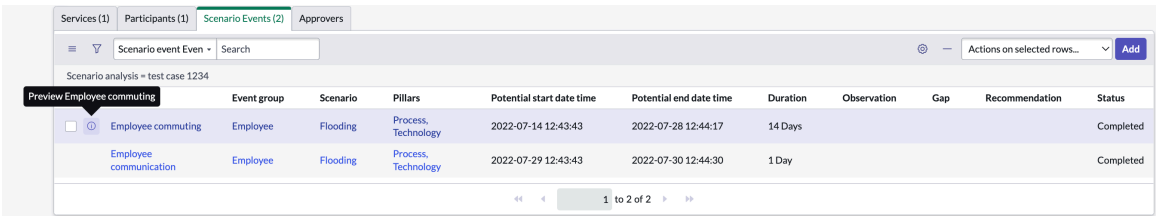

**10.** Add a scenario event to the scenario analysis.
You can associate one or more events to the scenario as shown in the following example.

### Add scenario events to an analysis




**11.** Click the scenario event and open its information record in the Scenario Events related list.
You can review the scenario event information record as shown in the following example.

### Scenario event information record

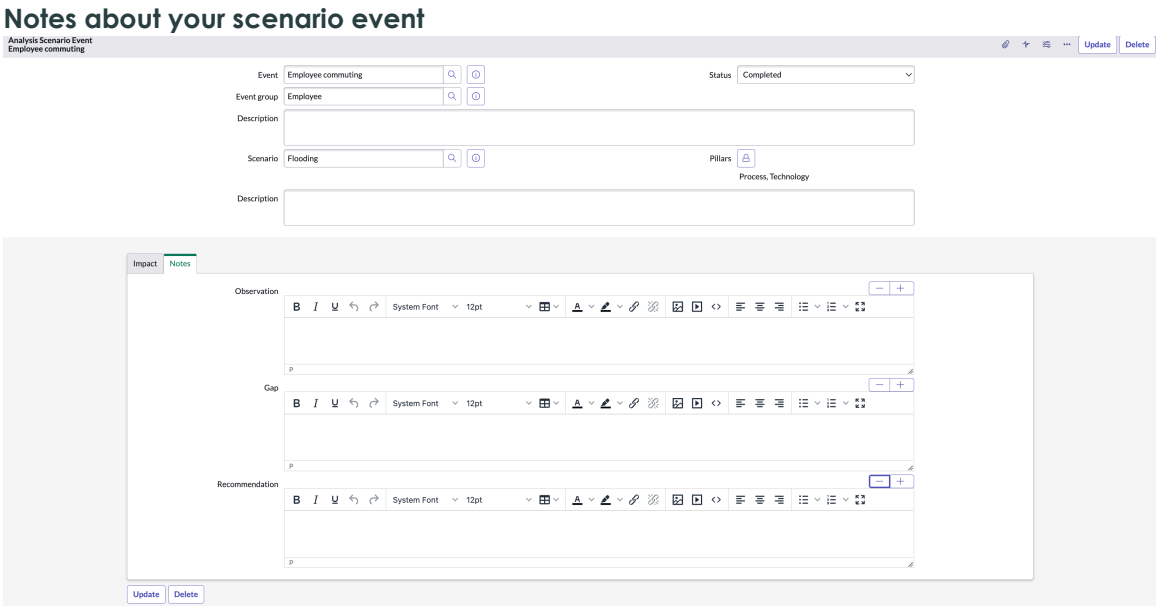



If you are the owner of the analysis, you can collect the observations, gaps, and recommendations from all the participants and update the information by performing the following tasks:

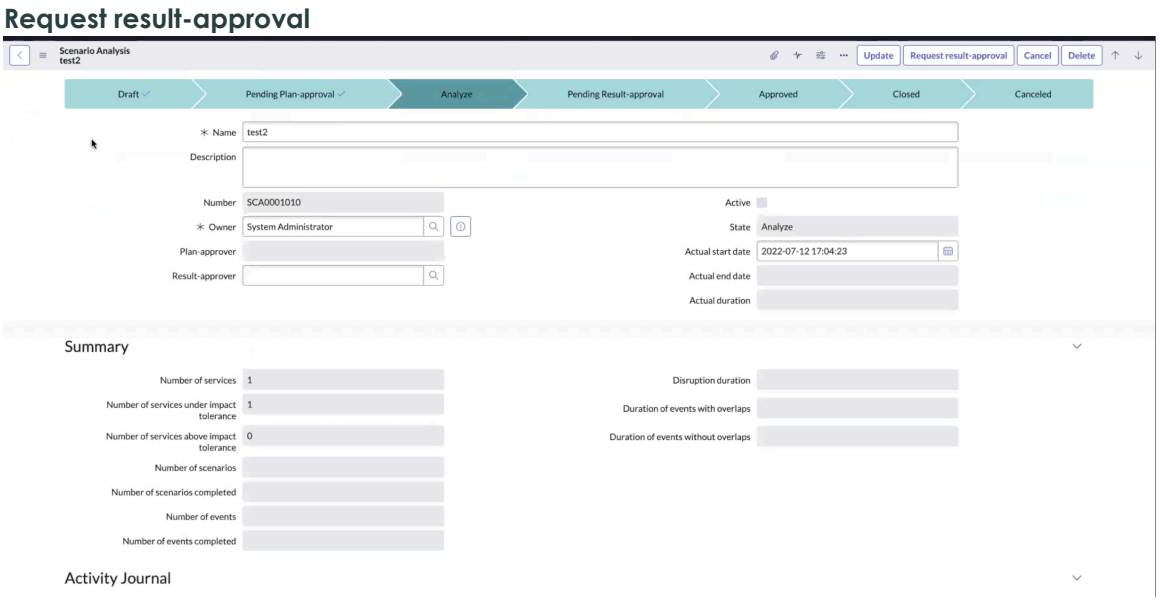
- In the Impact panel, review and update the dates and duration in the **Potential start date time**, **Potential end date time**, and **Duration** fields.
- In the Notes panel, add your observations, gaps, and recommendations about the scenario analysis event in the **Observation**, **Gap**, and **Recommendation** fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- To add your observations and recommendations in the application, click **Update** as shown in the following example.



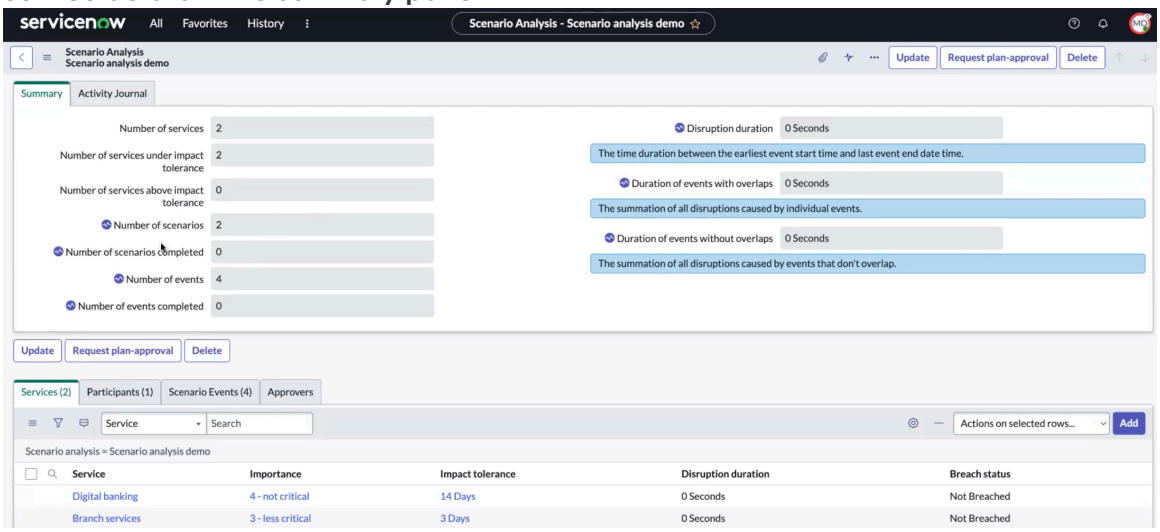

12. In the Events related list, close all the scenario events before you request the result approval.
13. Click **Request result-approval**.



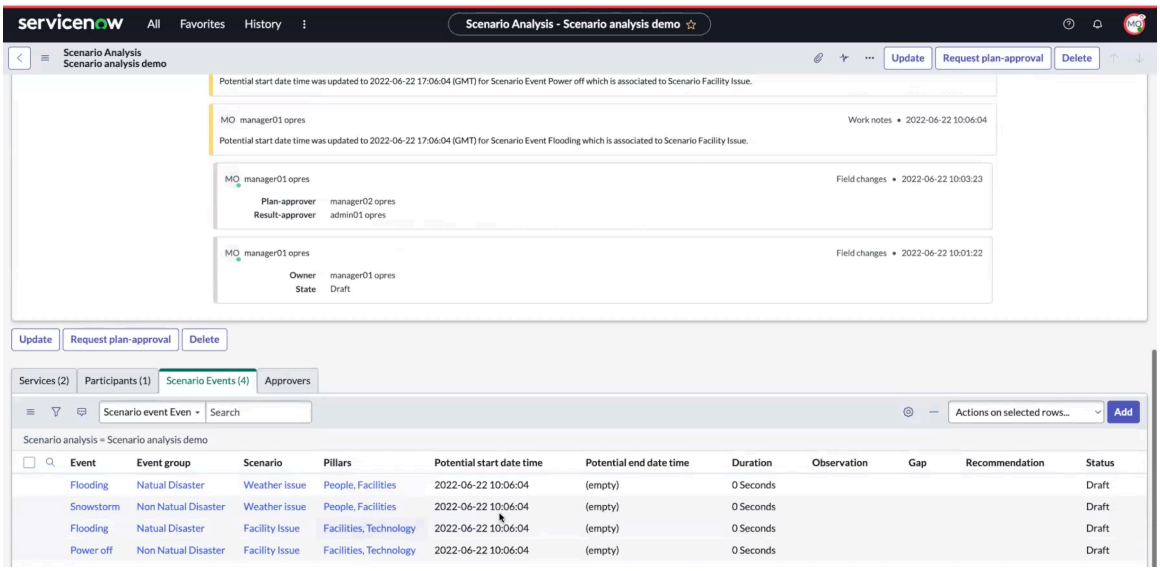

In the Summary and Activities panel of the Scenario Analysis form, the details about the service and work notes are updated as shown in the following examples.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Service details in the Summary panel




### Auditor activity and work notes in the Activities panel




14. Click **Request plan-approval**.

## Result

The scenario analysis that you have requested an approval for is displayed in the Scenario Analyses list view in the application UI.

### Scenario Analysis form

Use the Scenario Analysis form to add the details about the scenario. For example, you can add the plan approver, result approver, and duration of the scenario analysis.

## Scenario Analysis form

For a description of the field values, see the following table.

### Scenario Analysis form

| Field | Description |
|---|---|
| Name | Name of the scenario analysis. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Scenario Analysis form (continued)

| Field | Description |
|---|---|
| Description | Description for the scenario analysis. |
| Number | Number for the scenario analysis. When you create a scenario analysis, the application creates a scenario analysis record and assigns it a unique identification number. This field is auto-filled. |
| Owner | Owner of the scenario analysis. This field is auto-filled. |
| Active | Option to mark the scenario analysis as active. |
| State | State of the scenario analysis. This field is auto-filled. |
| Plan-approver | Plan-approver for the scenario analysis. For more information on the fields in the user record, see User record form reference. |
| Result-approver | Result-approver for the scenario analysis. For more information on the fields in the user record, see User record form reference. |
| Actual start date | Actual start date of the scenario analysis. |
| Actual end date | Actual end date of the scenario analysis. This field is auto-filled. |
| Actual duration | Actual duration of the scenario analysis. This field is auto-filled. |
| Summary | |
| Number of services | Number of services that are associated with the scenario analysis. |
| Number of services under impact tolerance | Number of services that are associated with the scenario analysis that are under impact tolerance. |
| Number of services above impact tolerance | Number of services that are associated with the scenario analysis that are above impact tolerance. |
| Number of scenarios | Number of scenarios that are associated with the analysis. |
| Number of scenarios completed | Number of completed scenarios that are associated with the analysis. |
| Number of events | Number of events that are associated with the analysis. |
| Number of events completed | Number of completed events that are associated with the analysis. |
| Disruption duration | Time duration between the end time of the last event and the start time of the first event. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Scenario Analysis form (continued)

| Field | Description |
|---|---|
| Duration of events with overlaps | Summation of all event durations including the overlapping events and pauses. |
| Duration of events without overlaps | Summation of all event durations without the overlapping events and pauses. |
| Activity Journal | |
| Work notes | Work notes for the activities that are related to the record. |
| Additional comments (Customer visible) | More comments that can be shared with the customer. |
| Related lists | |
| Services | Services that are associated with the scenario analysis. |
| Participants | Participants that are associated with the scenario analysis. |
| Scenario Events | Scenario events that are associated with the scenario analysis. In the Scenario analysis event record, a user with the sn_oper_res.manager role updates the following details:<br>• Impact Panel<br>◦ Potential start date time: Date and time when a user starts working on the event.<br>◦ Potential end date time: Date and time when a user finishes working on the event.<br>◦ Duration: Calculated duration of the event.<br>• Notes panel<br>◦ Observations: Observations about the scenario event.<br>◦ Gaps: Gaps or missing information about the scenario event.<br>◦ Recommendations: Recommendations about the scenario event. |
| Approvers | Approvers that are associated with the scenario analysis. |

## User New record form

### User record form reference

| Field | Description |
|---|---|
| User ID | User ID of the approver. |
| First name | First name of the approver. |
| Last name | Last name of the approver. |
| Title | Title of the approver. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**User record form reference (continued)**

| Field | Description |
|---|---|
| Department | Department of the approver. |
| Email | Email address of the approver. |
| Language | Language of the approver. Available options are as follows:<br>• None<br>• English |
| Calendar integration | Integration of the approver's calendar. Available options are as follows:<br>• None<br>• Outlook |
| Time zone | Time zone of the approver. Available options are as follows:<br>• System (America/Los Angeles)<br>• Canada<br>• Europe<br>• GMT<br>• Hongkong<br>• US |
| Date format | Date format for the email message. Available options are as follows:<br>• MM-dd-yyyy<br>• dd/MM/yyyy<br>• dd-MM-yyyy<br>• dd.MM.yyyy<br>• yyyy-MM-dd |
| Password needs reset | Option to enable a password reset. To set up the user's password, save the record and then click **Set Password**. |
| Locked out | Option to mark if the user account is locked out. |
| Active | Option to mark the user account as active. |
| Business phone | Business phone of the approver. |
| Mobile phone | Mobile phone of the approver. |
| Photo | Option to add a photograph of the user. |
| Web service access only | Option to mark if the user has web service access only. |
| Internal Integration User | Option to mark if the user is an internal integration user. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**User record form reference (continued)**

| Field | Description |
|---|---|
| Enable Multi-factor Authentication | Option to enable multi-factor authentication for the account. |
| Related links | |
| View linked accounts | Link to view the linked accounts for the approver. |
| View subscriptions | Link to view the subscriptions for the approver. |

## Check your email notification for approving the scenario analysis

Check your email notifications so that you can approve the scenario analysis as the administrator of the Operational Resilience application. The email notifications are set up as part of the automated workflow.

### Before you begin

Role required: sn_oper_res.admin

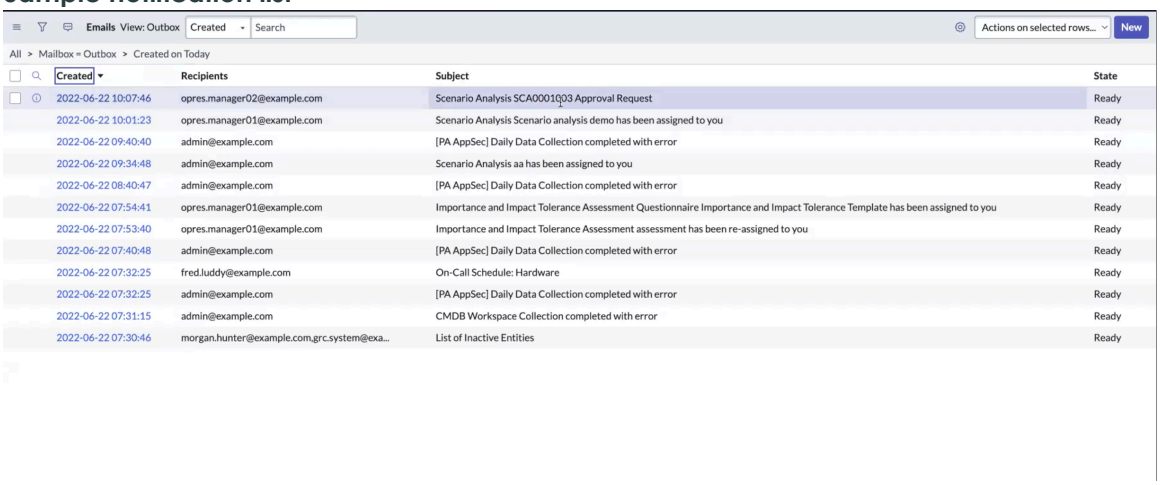
### About this task

When the analysis owner requests a plan-approval for the scenario analysis, you receive an email notification to approve or reject the scenario analysis. As an administrator of the application, you can approve or reject the scenario analysis. This task is optional.

### Procedure

1. Navigate to **All** > **Outbox**.
2. Locate the email notification that you have received for the scenario analysis.
   See the notification list as shown in the following example.

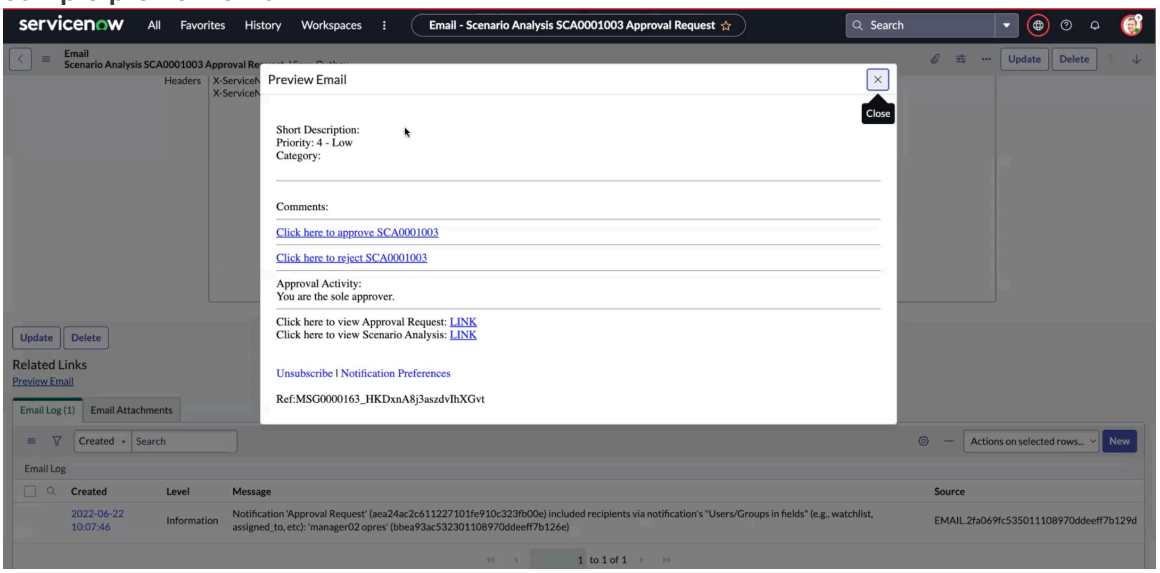
**Sample notification list**




3. Click the email notification and click **Preview email.**
   See the preview email as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Sample preview email




4. Click **Approve**.
   As an administrator of the Operational Resilience application, you can approve the scenario analysis.

## Close your scenario analysis

Update the status of the scenario event, request an approval, and close your scenario analysis as the last step of performing a scenario analysis of your services in the Operational Resilience application.

### Before you begin

Role required: sn_oper_res.manager

### About this task

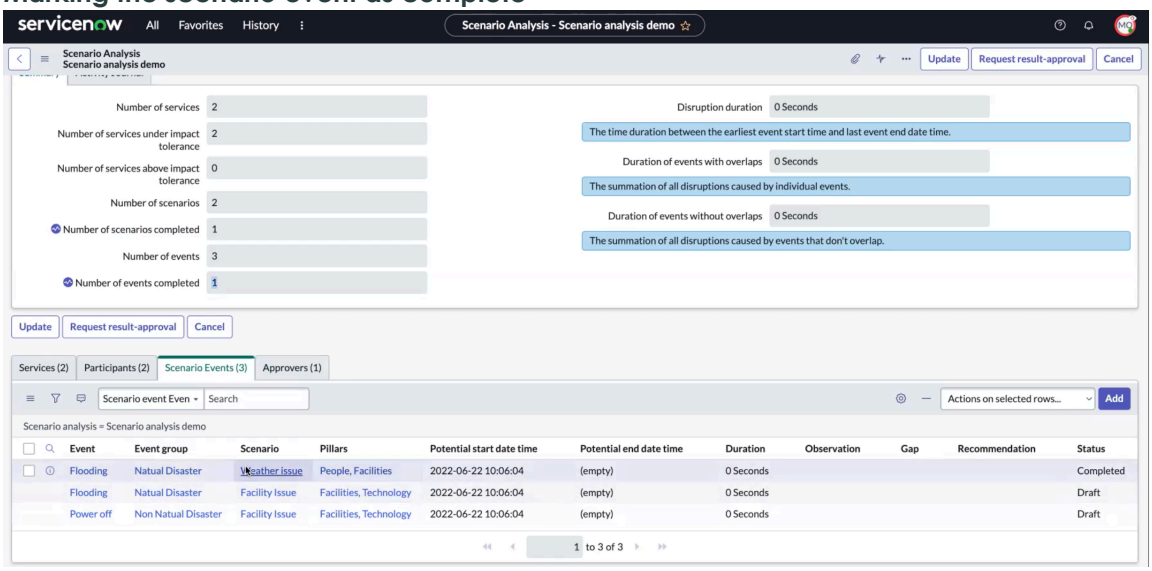
If you have the sn_oper_res.manager role, you can approve and close the scenario analysis as its owner.

### Procedure

1. To approve the scenario analysis, log in with the sn_oper_res.manager role as the plan-approver and click **Approve**.
2. To update the status of the scenario event as Complete in the Scenario events related list, log in as an owner of the scenario analysis.
   See the sample configuration in the Scenario events related list as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

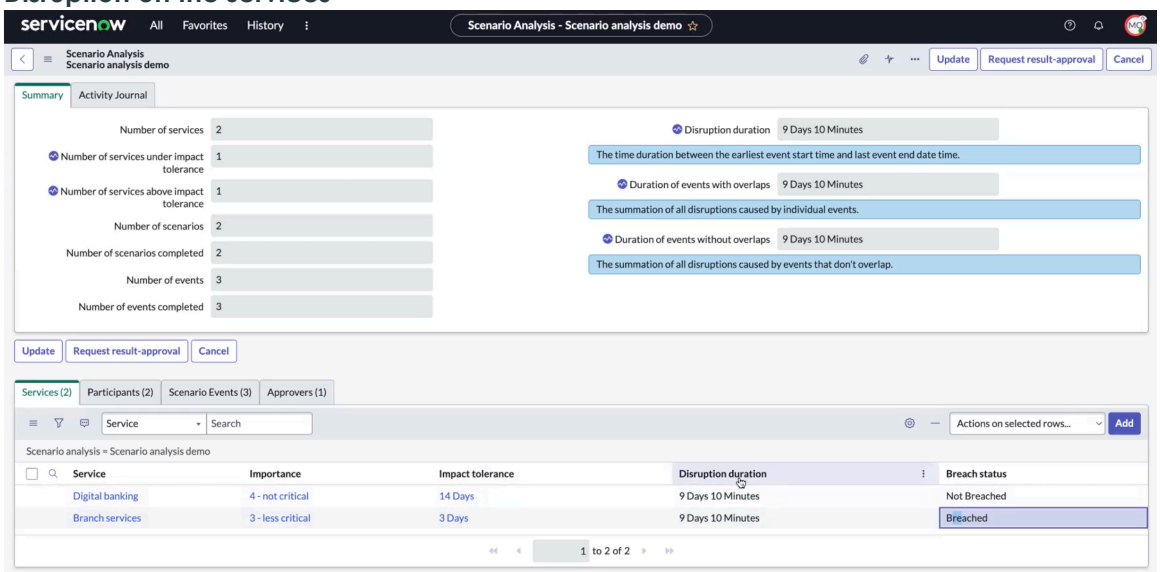
### Marking the scenario event as complete




**Note:** All scenario events must be marked as Complete before requesting the result approval.

3. Calculate the disruption on the services and determine if any service was breached.

### Disruption on the services



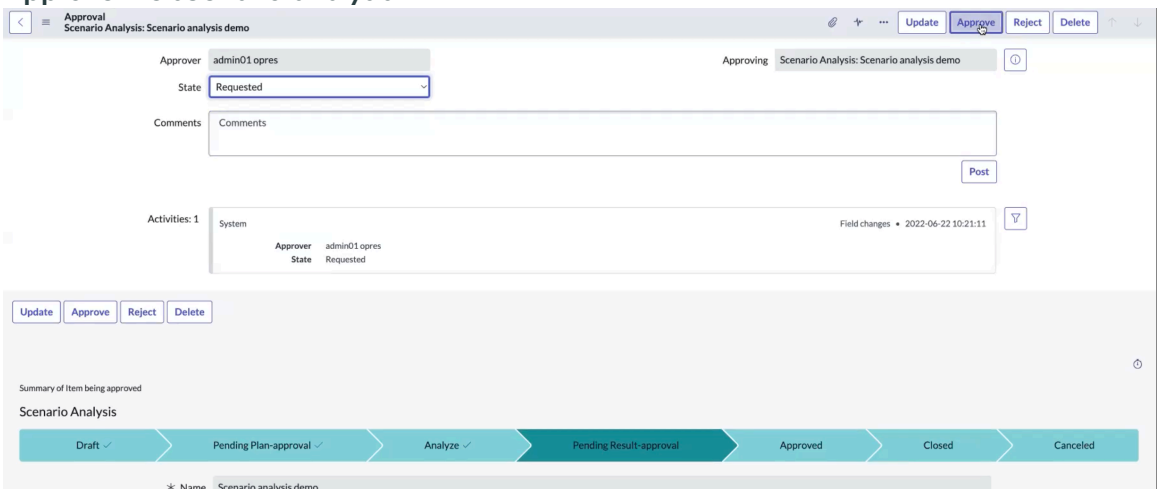

4. To request or approve the scenario analysis, log in as an owner of the scenario analysis and click **Request result-approval**.

**Note:** As an owner of the scenario analysis, you can update the services, participants, and scenario events before requesting the result-approval. After requesting the result-approval, the scenario analysis form is locked.

5. To approve the scenario analysis record, log in with the sn_oper_res.manager role as the approver of the scenario analysis, navigate to **My approvals**, open the scenario analysis record, and click **Approve**.
Approve the scenario analysis as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Approve the scenario analysis




You have moved the scenario analysis to the **Approved** state.

6. To close the scenario analysis record, log in as the approver of the scenario analysis, navigate to the scenario analysis record in the list view, and click **Close**.
   You have moved the scenario analysis to the **Closed** state. The Scenario Analysis form is locked and the scenario analysis workflow is complete.

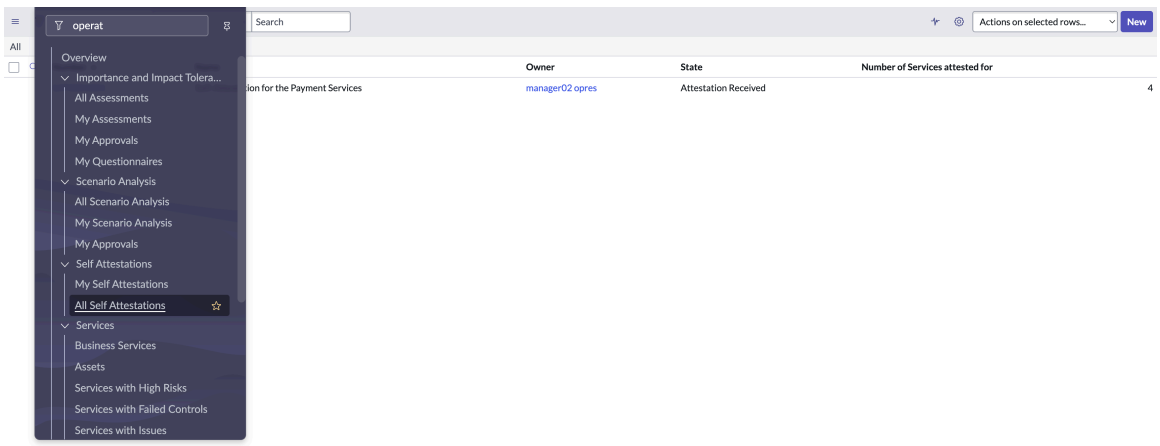
## Self-attesting the status of the business services

You can self-attest the status of the business services in the Operational Resilience application. By selecting the services and providing the answers to a pre-defined set of questions, you can complete the self-assessment and certify the operational resilience status of the services. You can sign, generate a self-attestation report, and upload a PDF so that you can have a copy of your report.

## Viewing your self-attestations

If you have the sn_oper_res.manager role, you can manage your attestations by navigating to the **All** > **Operational Resilience** > **Self Attestations** module in the application UI as shown in the following example.

### Self Attestations module




You can select the multiple services that you want to attest and submit an attestation for. To attest the status of the business services, use the following attestations modules that are listed under **All** > **Operational Resilience** > **Self Attestations**:

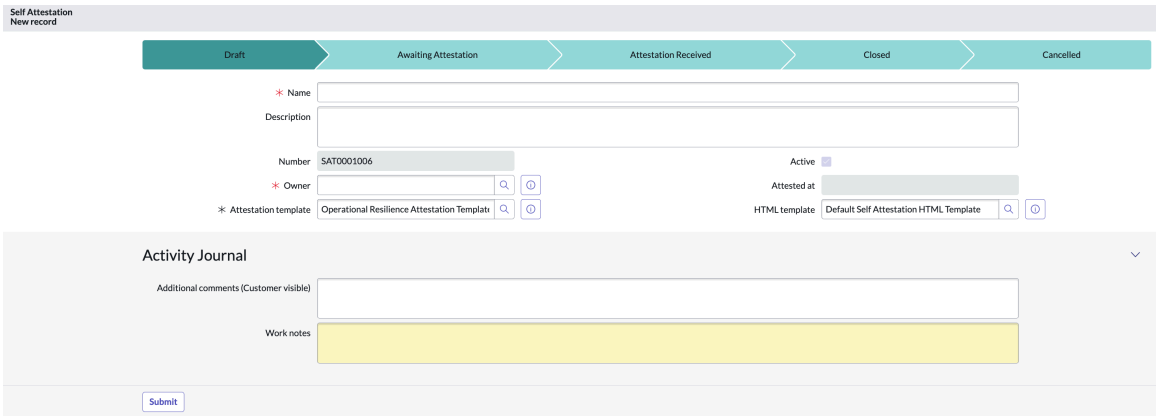
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **My Self Attestations**: Manage the self-attestations that are assigned to you.
- **All Self Attestations**: Manage and view all the self-attestations that are available in the system for the services.

## Using the self-attestation template

You can use the self-attestation template that is provided in the Operational Resilience application and create a self-attestation record as shown in the following example.

**Self-attestation record**




## Workflow and self-attestation states

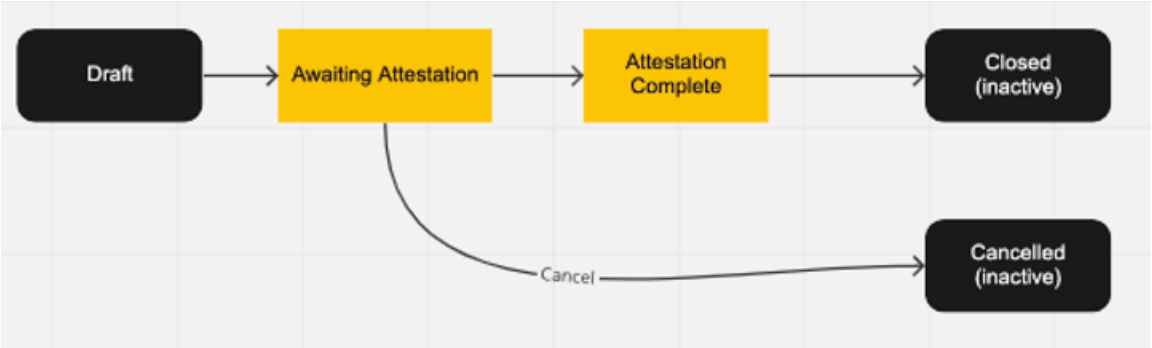
If you have the sn_oper_res.manager role, you can perform the following tasks in this workflow:

- Initiate a self-attestation to attest one or more business services.
- Select an attestation template on which the assessment takes place.
- Provide the details about the services, such as the service name and description, on the self-attestation form. You can also add the business services to attest from the related list in the record.
- Submit your services for self-attestation. This action creates an assessment instance for the user that has questions from the attestation template.
- Export the attestation to a PDF after you complete an assessment. You must use the HTML template that is provided in the self-attestation record. The HTML template provides the format for the PDF and an option to include your signature.
- Optionally, you can define an attestation template instead of using the default attestation template that is provided with the base system.

When you complete the self-attestation tasks, the states for the self-attestation are updated automatically in the Operational Resilience application as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Self-attestation process**




The states in the self-attestation process are explained in the following table.

**States that are associated with the self-attestation process**

| State | Description |
|---|---|
| Draft | A user with the sn_oper_res.manager role submits a self-attestation record. A record is created in the **Draft** state by default. |
| Awaiting Attestation | A user with the sn_oper_res.manager role selects an attestation template and associates the business services with the self-attestation record.<br><br>The application then creates an assessment instance automatically. This action moves the state of the self-attestation record to **Awaiting Attestation**. The assessment instance is displayed in the Assessment Instances related list in the UI. |
| Attestation Received | The owner of the self-attestation enters the responses to the different questions tin the attestation template and submits the answers. The state of the self-attestation is then updated automatically to **Attestation Received**. |
| Closed | The owner of the self-attestation record exports the questionnaire response to a PDF and signs the document. The state of the self-attestation is then updated to **Closed**. |
| Cancelled | If the self-attestation contains an invalid or incorrect data, a user with the sn_oper_res.manager role can cancel the self-attestation. The state of the self-attestation is then updated to **Cancelled**. |

## Reference information

For more information on submitting a self-attestation record, see Create a self-attestation record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For the description of the field values that are listed in the self-attestation form, see Self-Attestation New Record form.

As an optional task, you can create an attestation template instead of using the default attestation template that is provided with the base system. For more information on creating an attestation template, see Create and edit an attestation template.

### Create a self-attestation record

Create a self-attestation record for your business services in the Operational Resilience application. You can use the attestation template that is provided with the base system to create a self-attestation record.

#### Before you begin

Role required: sn_oper_res.manager

#### Procedure

1. Navigate to **All** > **Operational Resilience** > **Self Attestations** > **My Self Attestations**.
2. Click **New**.
3. In the Self-Attestation New Record form, enter the name of what you want to provide a self-attestation for.
4. In the **Owner** field, assign an owner for the self-attestation.
5. In the **Attestation Template** field, select the **Operational Resilience Attestation Template**.

   The attestation template contains the pre-defined questions for the assessment. Operational Resilience provides an attestation template as part of the base system. If you have the sn_oper_res.admin role, you can customize the default attestation template for your own business needs. Creating an attestation template is optional. For information on creating a customized attestation template, see Create a self-attestation record.

6. In the **HTML Template** field, select the **Default Self Attestation HTML Template**.
   The HTML template provides the format for the PDF and an option to include your signature in the attestation.
7. Click **Submit**.
   For the description of the field values on the form, see Self-Attestation New Record form.

#### Result

The self-attestation record is displayed in the Self Attestations list under My Self Attestations.

### Self-Attestation New Record form

If you're a user with the sn_oper_res.manager role, use the Self-Attestation New Record form to submit a self-attestation for your business services.

## Self-Attestation New Record form

For a description of the field values on the form, see the following table.

**Self-Attestation New Record form**

| Field | Description |
|---|---|
| Name | Unique name for the self-attestation record. |
| Description | Helpful information about the self-attestation record. |
| Number | Number for the self-attestation record. This field is auto-filled. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Self-Attestation New Record form (continued)**

| Field | Description |
|---|---|
| Owner | Label for the self-attestation record that is displayed in the UI. |
| Attestation template | Attestation template that is provided with the base system and that is used for creating the self-attestation. |
| Active | Option to mark the self-attestation record as active. |
| Attested at | Location where the attestation is certified. This field is auto-filled. |
| HTML template | Default self-attestation HTML template that is provided with the base system to export an attestation. The template has a pre-defined format, details of the answers, and services that have been attested for in the self-attestation report. |
| Activity Journal | Extra comments and work notes for the self-attestation. |

## Submit a self-attestation record

Submit a self-attestation record after you associate it with the relevant business services in the Operational Resilience application.

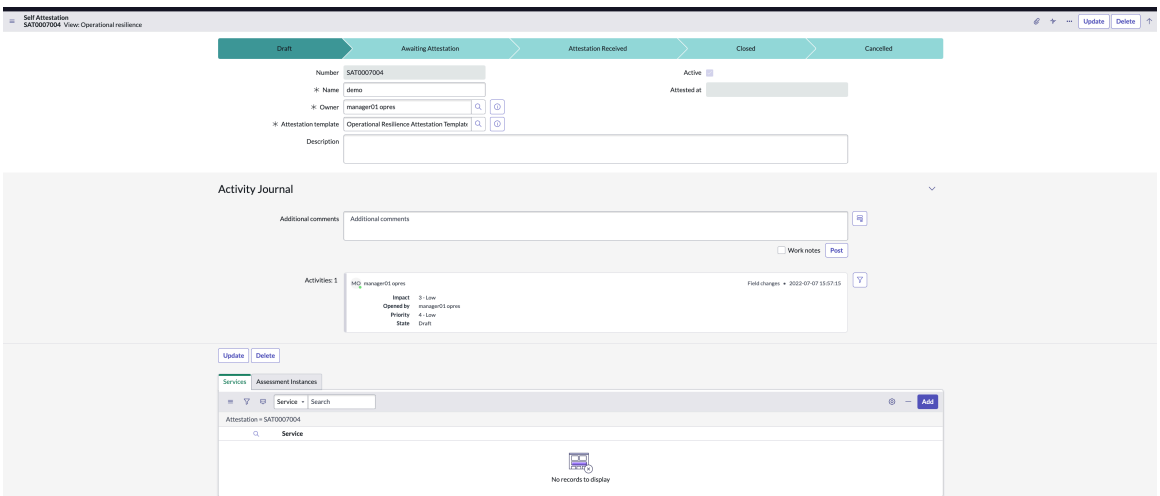
### Before you begin

Role required: sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience** > **Self Attestations** > **My Self Attestations** and select the self-attestation record that you are working on.
   The self-attestation record displays the Services related list as shown in the following example.

**Self-attestation record**




2. In the Services related list, click **Add**.
   Associate the relevant business services with your self-attestation.

**Note:** You can add only the critical services in the Services related list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

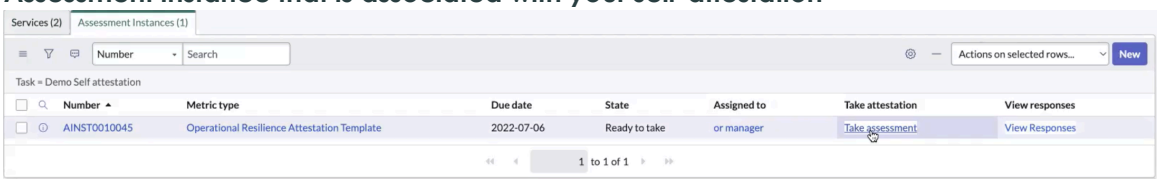
3. Select the services that you want to associate with the self-attestation record and click **Create Relationship**.
   The services that are associated with your self-attestation are displayed in the Services related list as shown in the following example.

**Services that are associated with your self-attestation**




4. In the self-attestation record, click **Submit for Self-Attestation**.
   When you submit the selected services for self-attestation, an assessment instance is created. This instance is displayed in the Assessment Instances related list as shown in the following example.

**Assessment instance that is associated with your self-attestation**




   This action moves the state of the self-attestation to **Awaiting Attestation**.

5. In the self-attestation record, click the assessment instance in the Assessment Instances related list.
6. Click **Take assessment**.
7. Respond to the questions in the assessment questionnaire.
   Respond to the questions as shown in the following example.

**Sample assessment**

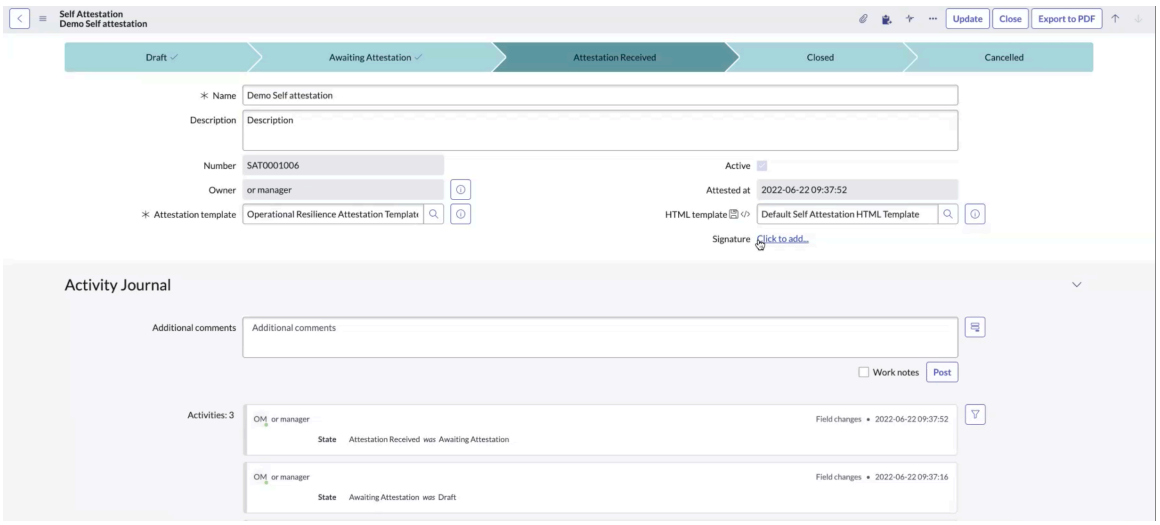



8. Click **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You have now updated the state of the self-attestation to **Attestation Received** as shown in the following example.

**Attestation Received state**




## Export your self-attestation to a PDF

Export the self-attestation to a PDF in the Operational Resilience application so that you can generate the self-attestation report.

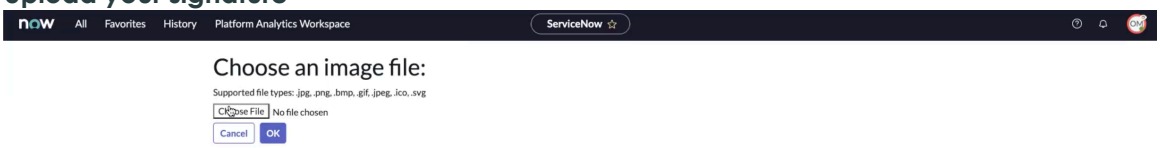
### Before you begin

Role required: sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience** > **Self Attestations** > **My Self Attestations** and open the self-attestation record where the self-attestation PDF is attached to the record.
2. In the **Signature** field, select **Click to add**.
3. Click **Choose File** and click **OK**.
   You can upload your signature for the self-attestation as shown in the following example.

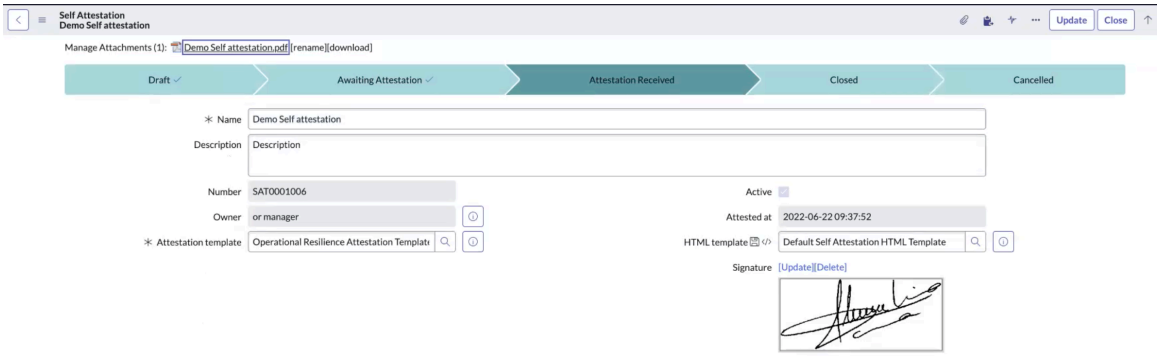
**Upload your signature**




4. Click **Export to PDF**.
   You have now exported the self-attestation PDF with the information about the associated business services. The PDF is displayed on the self-attestation record as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Self-attestation PDF




5. To download the self-attested PDF, click the **PDF** link in the Self Attestation form.
   The self-attested PDF displays the name, description, template, questions, and responses to the questions. It also displays a list of the services and the name, owner, importance, impact tolerance, and scenario analysis for the services.
6. Click **Close**.
   You have now moved the self-attestation to the **Closed** state. The self-attestation workflow is complete.

## Cancel a self-attestation record

Cancel an invalid or incorrect self-attestation record in the Self Attestation Record form in the Operational Resilience application. This way, you can remove records that are no longer valid and correct errors in the Self Attestation Record.

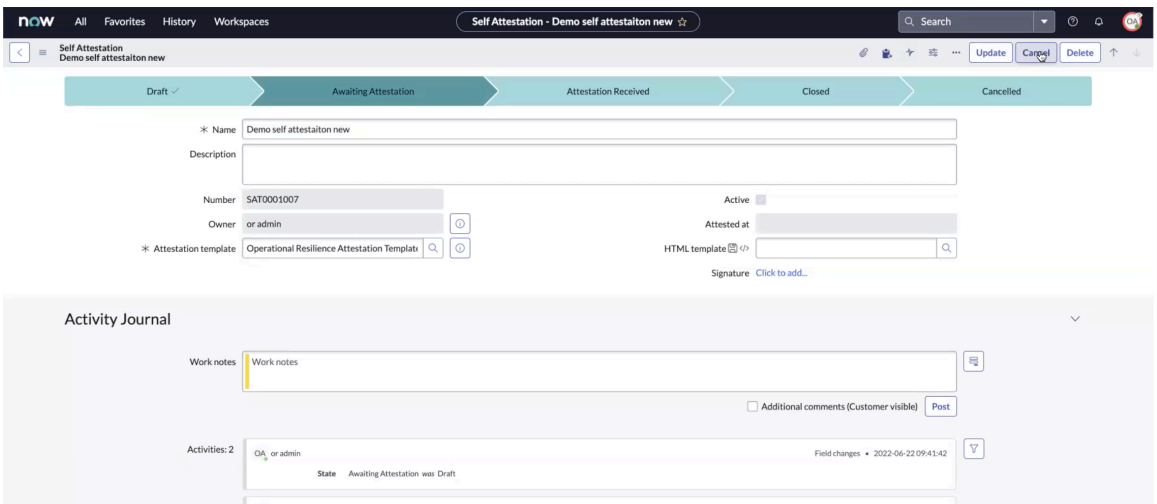
### Before you begin

Role required: sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience** > **Self Attestations** > **My Self Attestations**.
2. Select an attestation that you want to cancel from the Self Attestations list and click **Cancel**.
   An attestation may contain a wrong template or some erroneous details and you may have to cancel it as shown in the following example.

### Cancel a self-attestation




You have now canceled the self-attestation and removed it from the Self Attestations list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Setting up the features in Operational Resilience Workspace

Starting with GRC version 16.x.x, a new workspace has been introduced for the GRC: Operational Resilience application. You can use Operational Resilience Workspace for managing your resilience tasks and monitoring the resilience metrics from a single dashboard.

## Overview of Operational Resilience Workspace

Operational Resilience Workspace provides a single-pane view for an improved User Experience (UX) and a simplified user journey. The highlights of Operational Resilience Workspace are as follows:

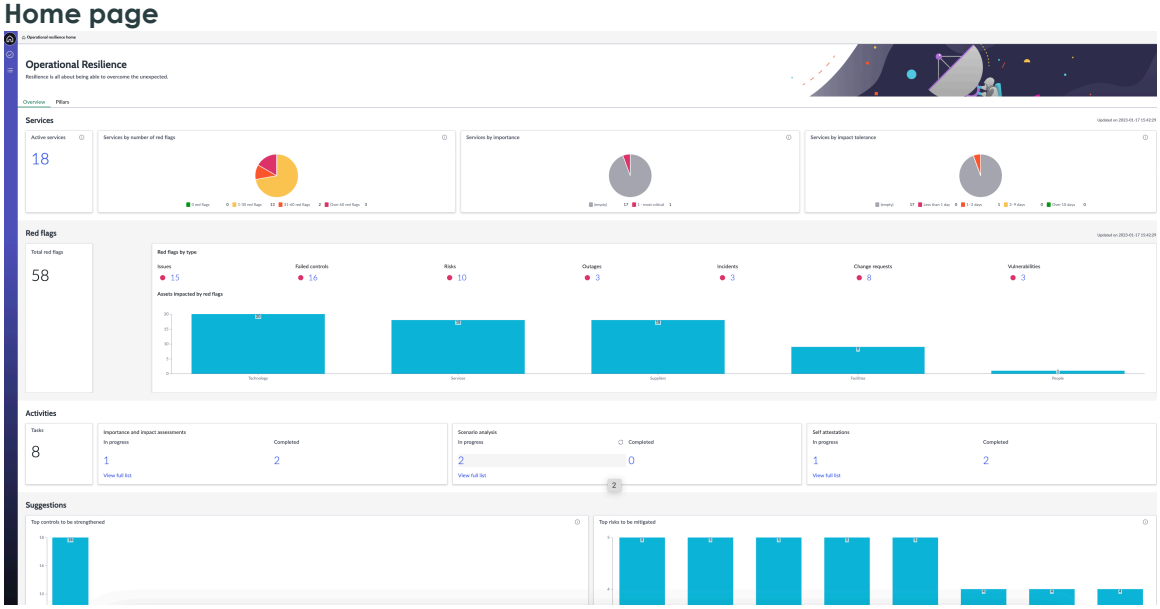
- Configure the resilience tasks by using the interactive forms.
- Visualize the resilience metrics on the dashboard.
- Track the risks, controls, and issues from the GRC applications on the related tabs in the Service form.
- Remediate the incidents, outages, vulnerabilities, and change requests for a business service.

You can view the data visualization components of the resilience metrics on the following pages:

- Home page: The Home page displays the status of the services and the pillars on the dashboard.
- Tasks page: The Tasks page displays your individual tasks and your team's tasks on the dashboard.
- List page: The List page displays the configurable resilience tasks, such as the importance and impact tolerance assessment or a scenario analysis in the list format.

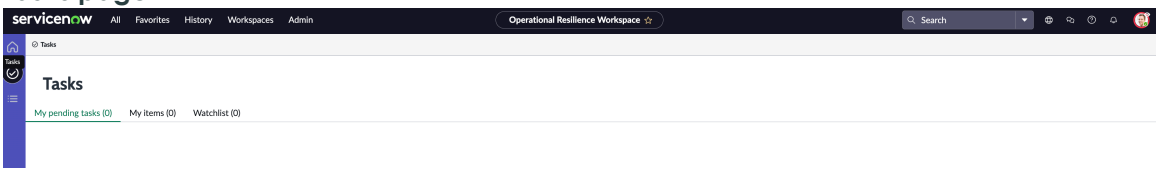
The Home page, Tasks page, and List page are displayed in the following examples.

### Home page

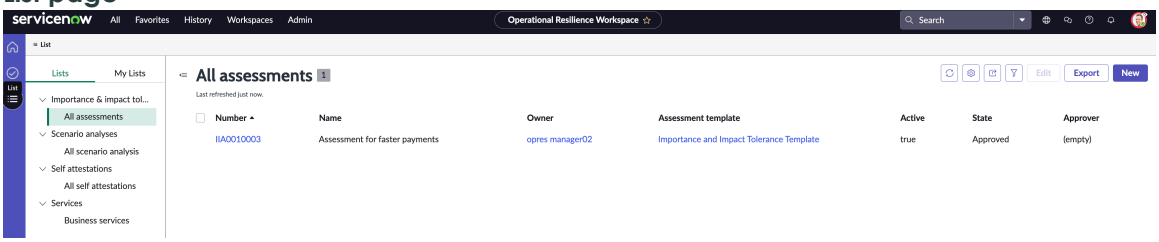



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Tasks page




### List page




## Roles required to access Operational Resilience Workspace

You can access Operational Resilience Workspace with the following user roles:

- Operational Resilience administrator [sn_oper_res.admin]
- Operational Resilience manager [sn_oper_res.manager]
- Operational Resilience user [sn_oper_res.user]

**Note:** For information on the administrative tasks, see Setting up the administrative tasks.

## Configurable features in Operational Resilience Workspace

You can configure the following Operational Resilience features in Operational Resilience Workspace:

- Importance and impact tolerance assessments
- Scenario analyses
- Self-attestations
- Business services

**Note:** As a user of the Operational Resilience application, you can customize your Operational Resilience Workspace experience by navigating through the UI messages and the tabs. If you add, delete, or change the order of the tabs, you may experience potential navigational errors in the Operational Resilience application UI.

## Exploring the Home page

The Home page in Operational Resilience Workspace provides a single-pane view on the status of the services and pillars in your organization. You can view the resilience metrics for a service, such as the operational status, completed activities, red flags, and suggestions for improving the metrics.

## Tabs in the Home page

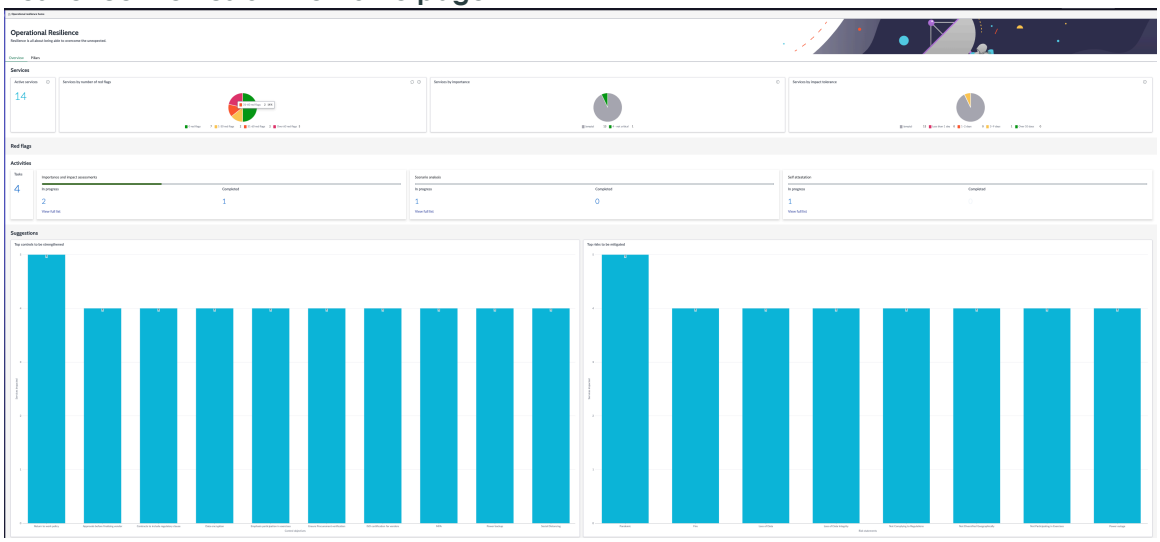
The Home page in Operational Resilience Workspace displays the following tabs:

- **Overview** tab—Displays an overview of the status of the services in your organization.
- **Pillars** tab—Displays the status and metrics of the pillars in your organization.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following example shows the resilience metrics for a service on the Home page.

### Resilience metrics on the Home page



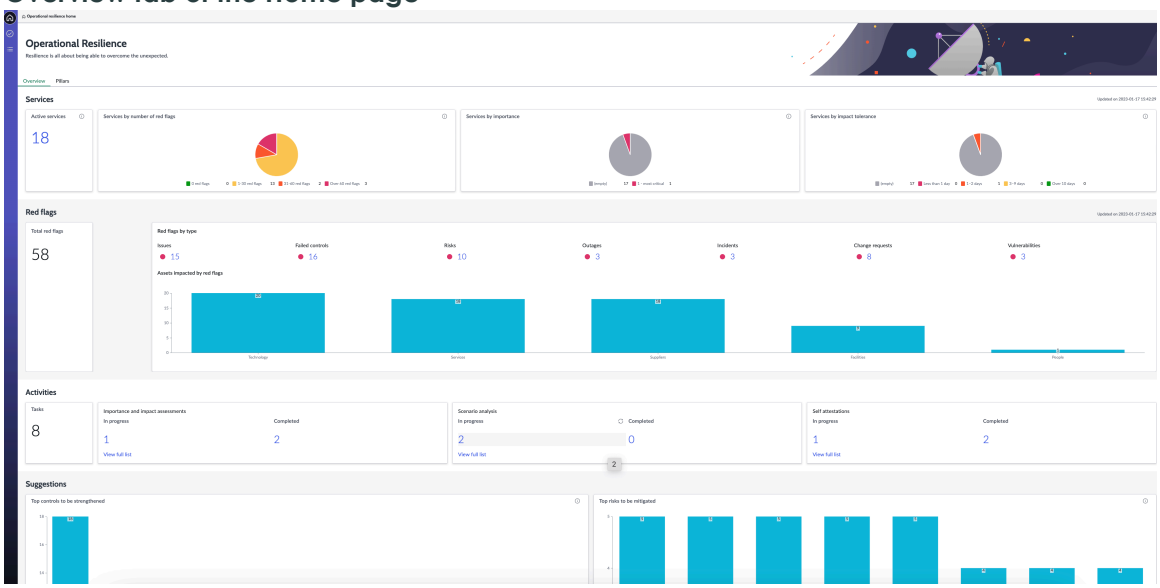

## Overview tab

On the **Overview** tab of the Home page, you can review a summary of the services in the following sections:

- Services
- Red flags
- Activities
- Suggestions

A sample **Overview** tab is shown in the following example.

### Overview tab of the Home page




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:**

As an administrator, you can navigate to **System properties > All properties** in your instance and configure the *sn_oper_res.red_flags_exclusion* property for the red flags section. You can configure the child tables of the *sn_oper_res_service_process_pillar* table that should be not considered as part of the red flags section.

By default, the services tasks, Business Continuity Management plan (Crisis events), and Dependencies (Assets) are excluded from the display list in the Red flags section.

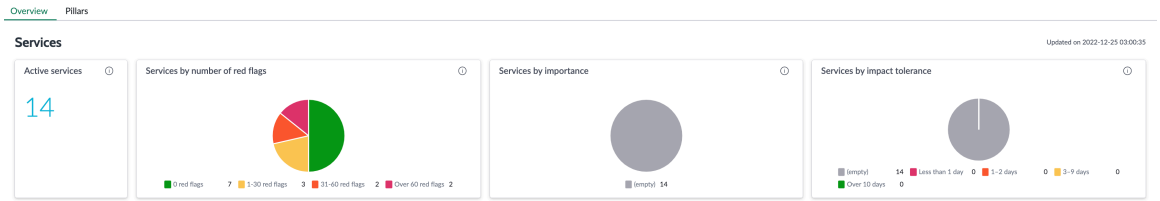
## Services section

In the Services section on the **Overview** tab, you can review the following details on the services:

- Active services
- Services by number of red flags
- Services by importance
- Services by impact tolerance

A sample Services section is shown in the following example.

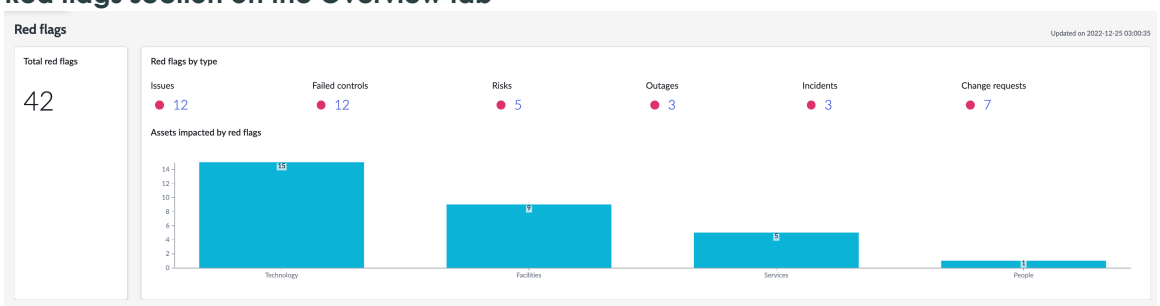
**Services section on the Overview tab**




## Red flags section

In the Red flags section on the **Overview** tab, you can review the services that have been flagged for alerts as shown in the following example.

**Red flags section on the Overview tab**




You can view the following sample details on the red flags for a service:

- Total red flags: You can view the total number of the red flags that are applicable for a service.
- Red flags by types: You can view the red flags for a service that are classified by the following types.
  - Issues
  - Failed controls

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

  - Risks
  - Outages
  - Incidents
  - Change requests
- Assets impacted by red flags: You can view the assets such as the Technologies and Facilities pillars that are impacted by the red flags.

## Displaying reports for different user roles

Separate reports are displayed in the Operational Resilience Workspace Home page for BCM Professional and IRM Professional users.

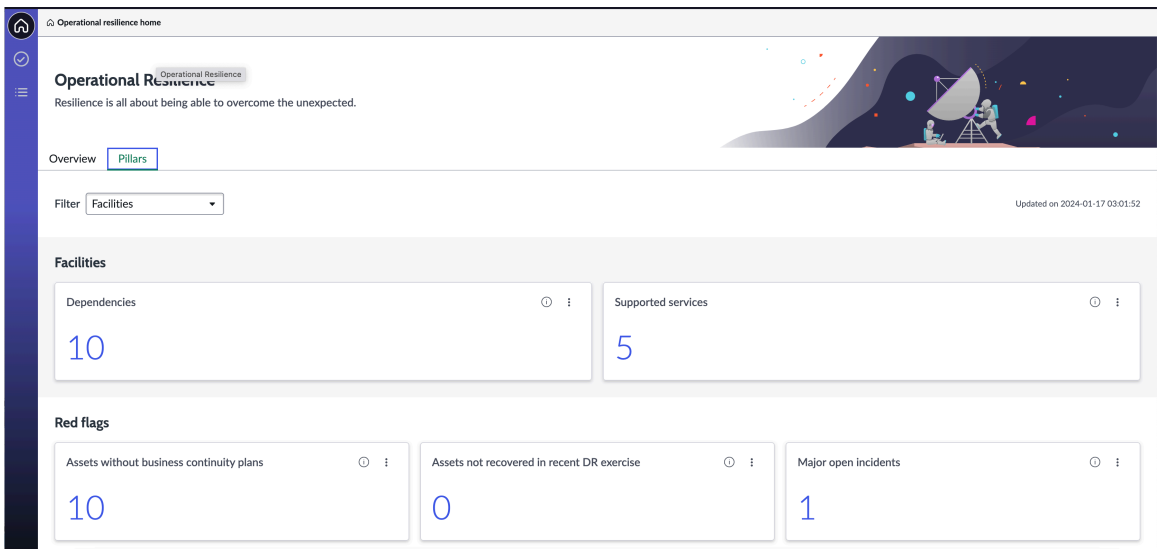
## Enhanced roles for accessing the reports

The roles installed with Operational Resilience now contain the relationship for BCM Professional and IRM Professional users.

The system administrators, Operational Resilience managers, and Operational Resilience users can access all reports from the BCM and IRM applications in the Home page.

A user with the following roles can access the BCM reports in the Operational Resilience Workspace as shown in the example.

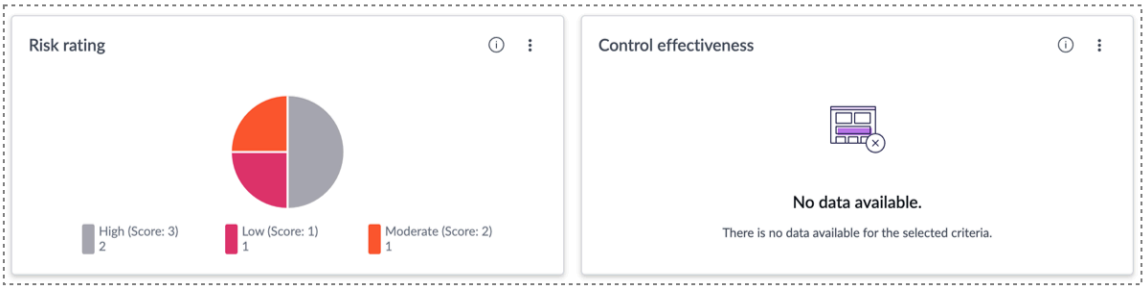
- sn_oper_res.bcm_opres_admin
- sn_oper_res.bcm_opres_manager
- sn_oper_res.bcm_opres_user




A user with the following roles can access the IRM reports in the Operational Resilience Workspace as shown in the example.

- sn_oper_res.irm_opres_admin
- sn_oper_res.irm_opres_manager
- sn_oper_res.irm_opres_user

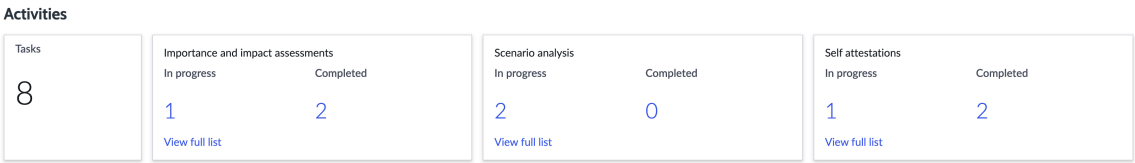
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## Activities section

In the Activities section on the **Overview** tab, you can view the status of the Operational Resilience tasks that are associated with a business service. You can view the in-progress tasks and completed tasks for an assessment or a scenario analysis as shown in the following example:

### Activities section on the Overview tab




In the Activities section on the **Overview** tab, you can review the following sample tasks that are associated with your services:

- Total number of tasks
- Importance and impact assessments
- Scenario analysis
- Self-attestation

## Suggestions section

In the Suggestions section on the **Overview** tab, you can view the system-generated suggestions for achieving better resilience metrics on the impacted services.

In the following example, the graph for the control objectives shows how the top controls can be strengthened for the impacted services. The graph for the risk statements shows how the top risks can be mitigated for the impacted services.

### Suggestions section on the Overview tab




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Pillars that are associated with a service

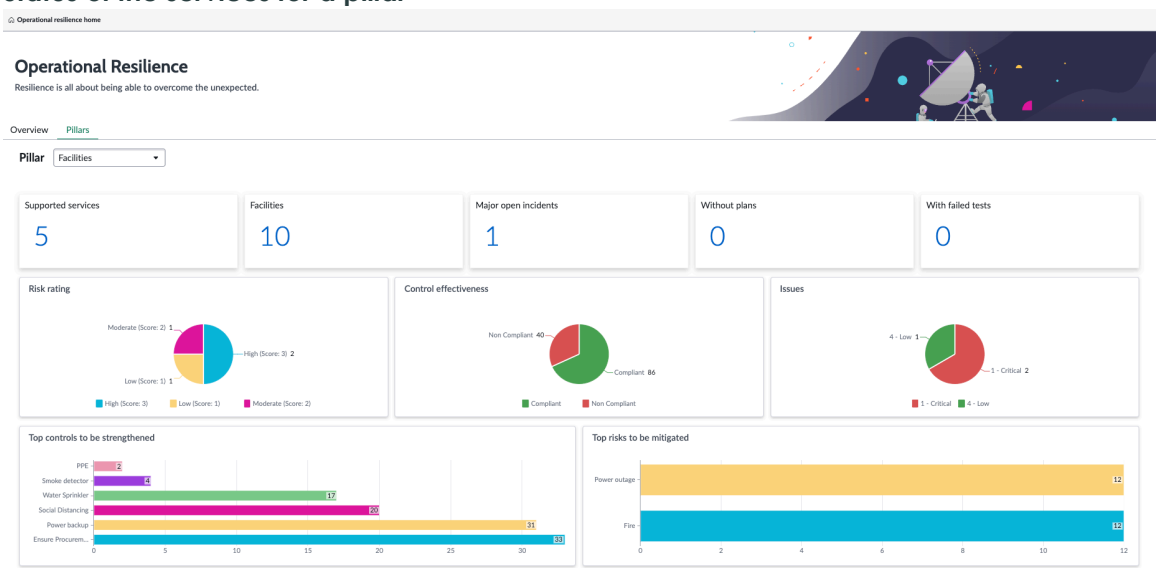
A pillar is a foundational block that contributes to the operational resilience of your organization. You can map the business services and processes to the pillars in the Operational Resilience application so that you can establish a relationship between these entities and monitor their status on the dashboard.

The Operational Resilience application provides the following pillars as part of the base system:

- Facilities
- People
- Suppliers
- Services
- Processes
- Technology

You can monitor the status of the services for each pillar. On the **Pillars** tab, the data that is associated with each pillar is displayed. The following example shows the controls, risks, and issues that are associated with a service for the Facilities pillar.

### Status of the services for a pillar




If you install the optional applications from the GRC product suite, such as Business Continuity Management and Vulnerability Response in your instance, you can also view the Business Continuity plan and Vulnerability Response reports on the dashboard.

For more information on the pillars, see Exploring Operational Resilience.

## Exploring the Tasks page and List page

The Tasks page in Operational Resilience Workspace provides a single-pane view of your pending tasks, your group's tasks, and the tasks that are on your watchlist. You can also update the tasks directly from the dashboard. On the List page, you can configure your operational resilience tasks.

## Tabs in the Tasks page

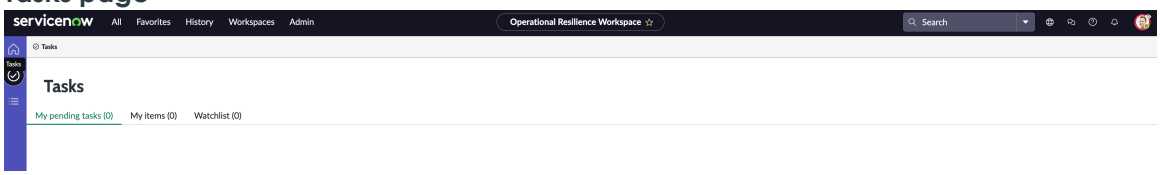
The Tasks page in Operational Resilience Workspace displays the following tabs:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **My pending tasks**
- **My items**
- **Watchlist**

A sample Tasks page for a logged-in user is shown in the following example.

**Tasks page**




## My pending tasks

The **My pending tasks** tab displays an overview of the pending tasks that are assigned to you and the tasks that require an action from you.

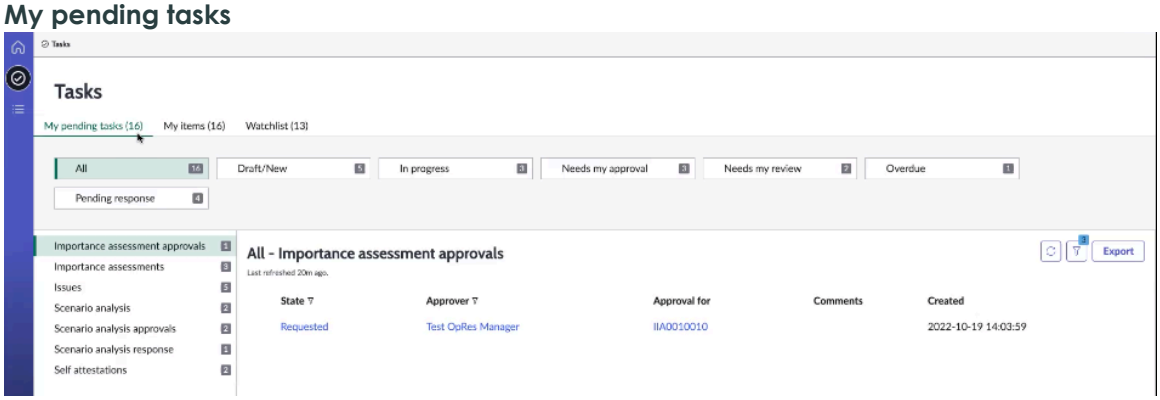
**Note:** The data displayed in the Tasks page is based on the roles of the users.

The **My pending tasks** tab displays your pending tasks in different states. You can filter your pending tasks by using the following types of the states:

- All
- Draft/New
- In progress
- Needs my approval
- Needs my review
- Overdue
- Pending response

The following example shows the pending tasks for the signed-in user.

**My pending tasks**

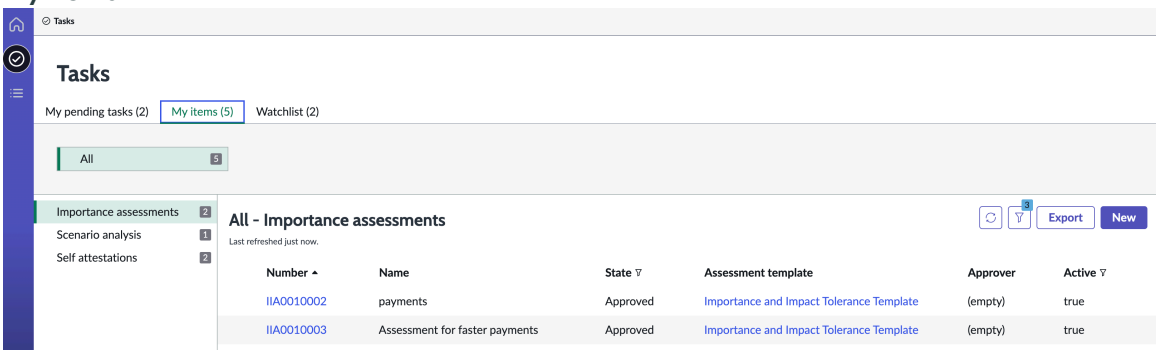



## My items

The **My items** tab displays a list of the tasks that are assigned to the signed-in user, such as the Operational Resilience Manager as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

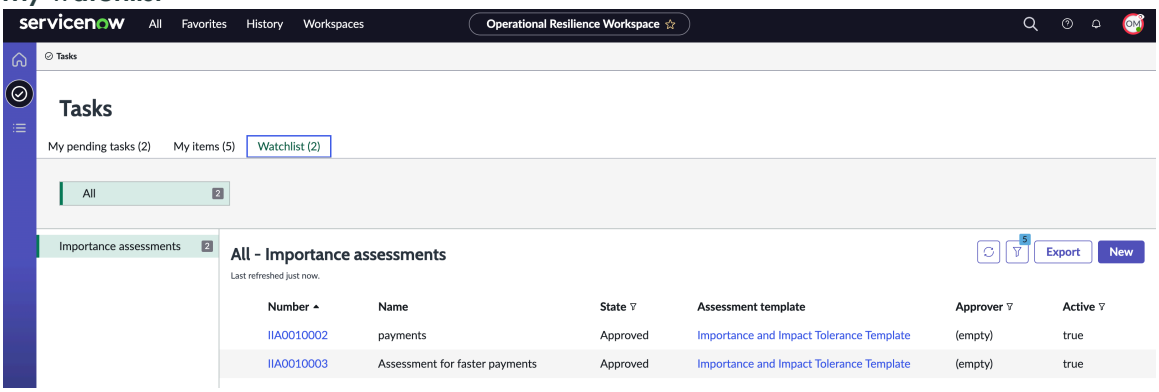
My items




## Watchlist

The **Watchlist** tab displays a list of the tasks that are on your watchlist. When a task is approved or completed, you receive a notification on the tab. The following example shows the updates on the assessments tasks that are on the signed-in user's watchlist.

My watchlist




**Note:** On the **My pending tasks**, **My items**, and **Watchlist** tabs, you can only view the records that are in-progress. On the **My pending tasks**, **My items**, and **Watchlist** tabs, the closed and canceled records aren't displayed. In Operational Resilience Workspace, you can view the closed and canceled records on their respective forms.

If you have the Operational Resilience administrator role, you can customize Operational Resilience Workspace by updating the Tasks page configurations. To update the Tasks page configurations, you can navigate to **All > GRC Landing Page Configurations > Tasks Page Configuration** in your instance.

If you have the Operational Resilience manager or Operational Resilience user roles, you can also get relevant recommendations on your resilience tasks on the Home page.

To view more information on the Tasks Page Configuration, see Update the Tasks Page Configuration record.

## List page in Operational Resilience Workspace

On the List page, you can set up a business service, analyze its importance and impact tolerance, perform a scenario analysis, and generate a self-attestation report.

For more information on setting up a business service in Operational Resilience Workspace, see Setting up your business services in Operational Resilience Workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information on analyzing the importance and impact tolerance of a business service in Operational Resilience Workspace, see Analyzing the importance and impact tolerance of a business service in Operational Resilience Workspace.

For more information on performing a scenario analysis in Operational Resilience Workspace, see Performing a scenario analysis in Operational Resilience Workspace.

For more information on self-attesting your business services in Operational Resilience Workspace, see Self-attesting the business services in Operational Resilience Workspace.

## Setting up your business services in Operational Resilience Workspace

You can set up your business services in Operational Resilience Workspace and monitor the resilience metrics on the dashboard. The Service form consolidates the attributes, risks, issues, control failures, and other areas of a business service that need attention.

## Overview of business services, parent services, and child services

A business service is a service that performs a business-level function. For example, you can use email, IT services, e-commerce, and telephone banking as business services that perform the business-specific functions in your organization.

You can classify a business service as a parent service and a child service. A parent service is a broad entity that you can use to service a business function. A parent service may contain its own subentities. A child service inherits its properties from the parent service. For example, the Payments service is a parent service and Mortgage payment or Maintenance payment are its child services.

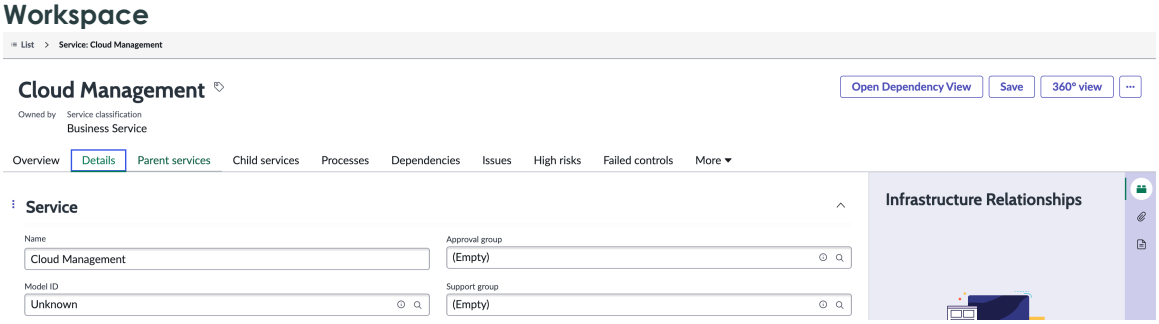
## Managing the business services in Operational Resilience Workspace

The Operational Resilience managers and users can access Operational Resilience Workspace. If you have the Operational Resilience managers and user roles, you can manage the business services and collect the resilience metrics in Operational Resilience Workspace.

## Configuring the parent services, child services, and processes in Operational Resilience Workspace

In Operational Resilience Workspace, you can configure the parent services, child services, and processes for a business service by using the **Parent services**, **Child services**, and **Processes** tabs directly. The sample tabs in the Service form are shown in the following example.

### Parent services, Child services, and Processes tabs in Operational Resilience Workspace

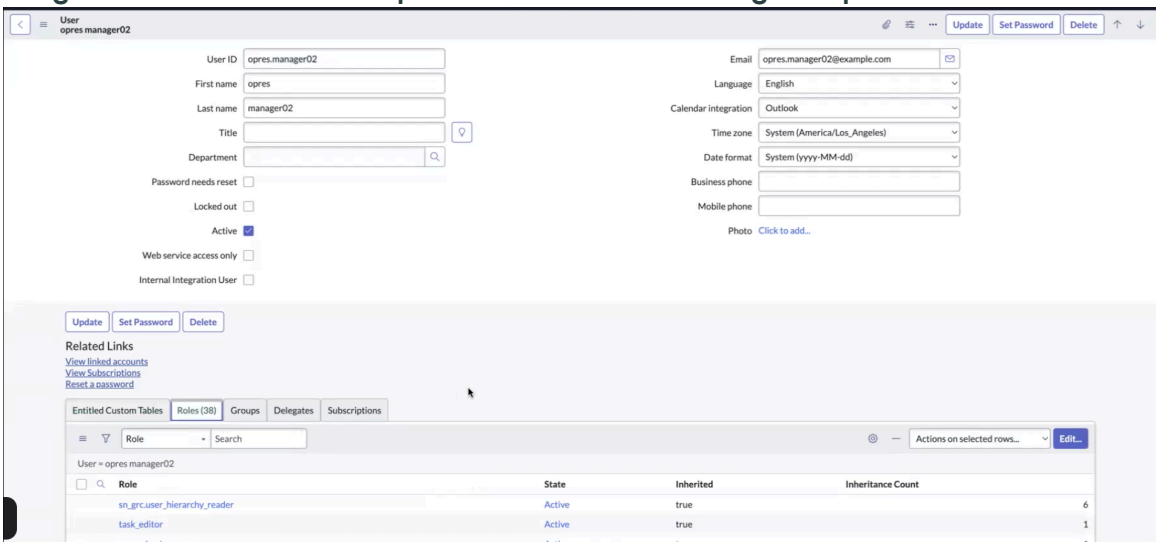



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

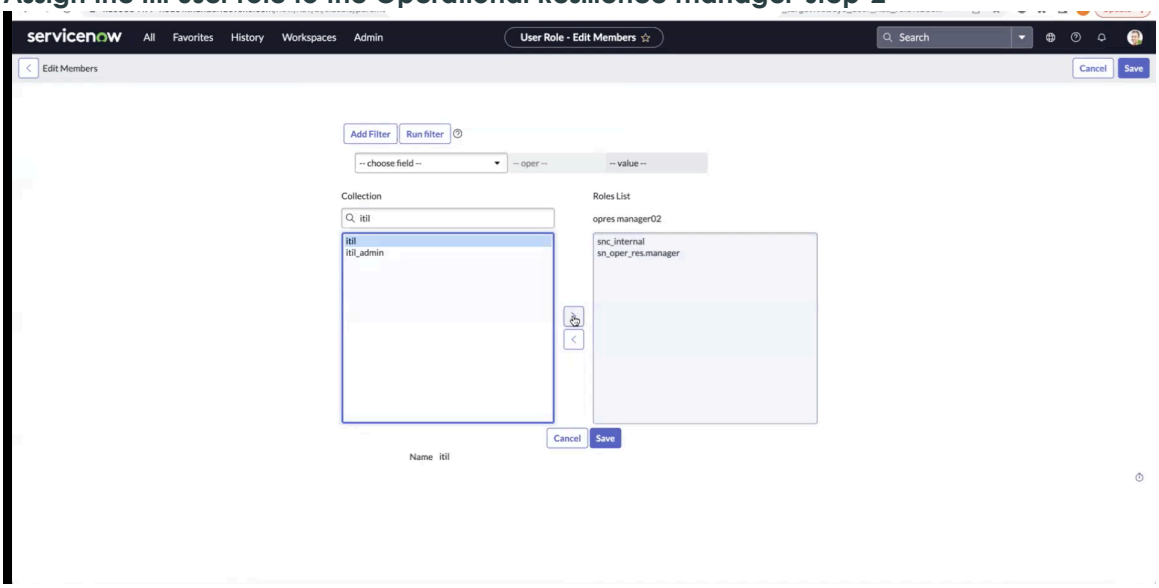
## Assigning the itil user role to the Operational Resilience administrators or managers

To configure the parent services, child services, or processes for a service, you must assign the itil user role to the Operational Resilience administrators or managers as shown in the following two steps.

### Assign the itil user role to the Operational Resilience manager-step-1




### Assign the itil user role to the Operational Resilience manager-step-2




### Note:

You must have the sn_oper_res.manager and itil role or the sn_oper_res.admin and itil role before you can add or remove the services and processes in Operational Resilience Workspace. In CMDB, granting any user with the itil role directly or indirectly allows the user to add or remove the services and processes from the backend. However, the Operational Resilience application prevents the users with the sn_oper_res.user role from adding or removing the services and processes in Operational Resilience Workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Adding a business service to Operational Resilience reporting

To add a business service to Operational Resilience reporting, you can select **Add to OpRes reporting** as shown in the following example.

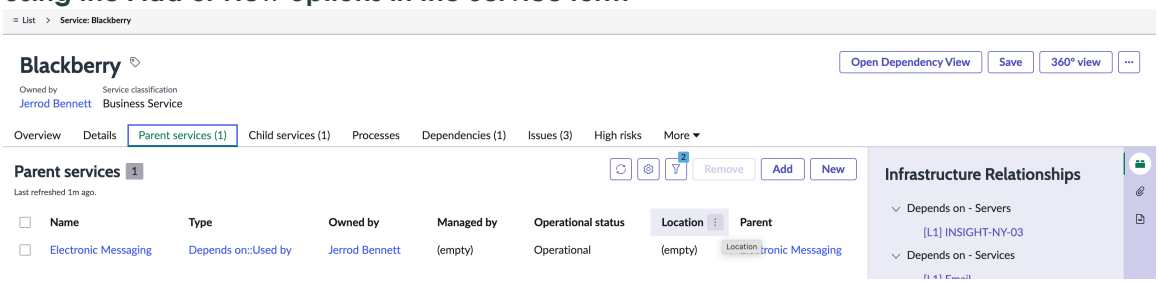
### Add a business service to OpRes reporting




**Note:** After you've added a service to Operational Resilience reporting in Operational Resilience Workspace, the **Add to OpRes reporting** option isn't displayed for the service anymore.

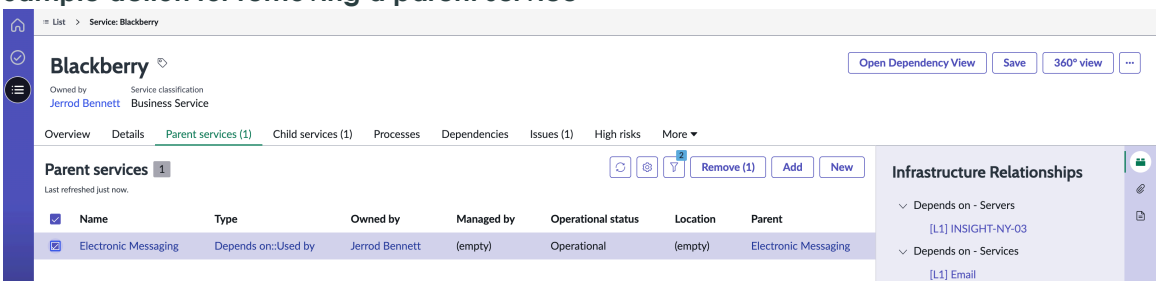
After adding a business service to Operational Resilience reporting, you can view the **Add** or **New** options in the Service form. To configure the relationship of a business service with its entities, you can use the **Add** or **New** options as shown in the following example.

### Using the Add or New options in the Service form




To remove an associated service or a process, select the service or the process and select **Remove** as shown in the following example.

### Sample action for removing a parent service

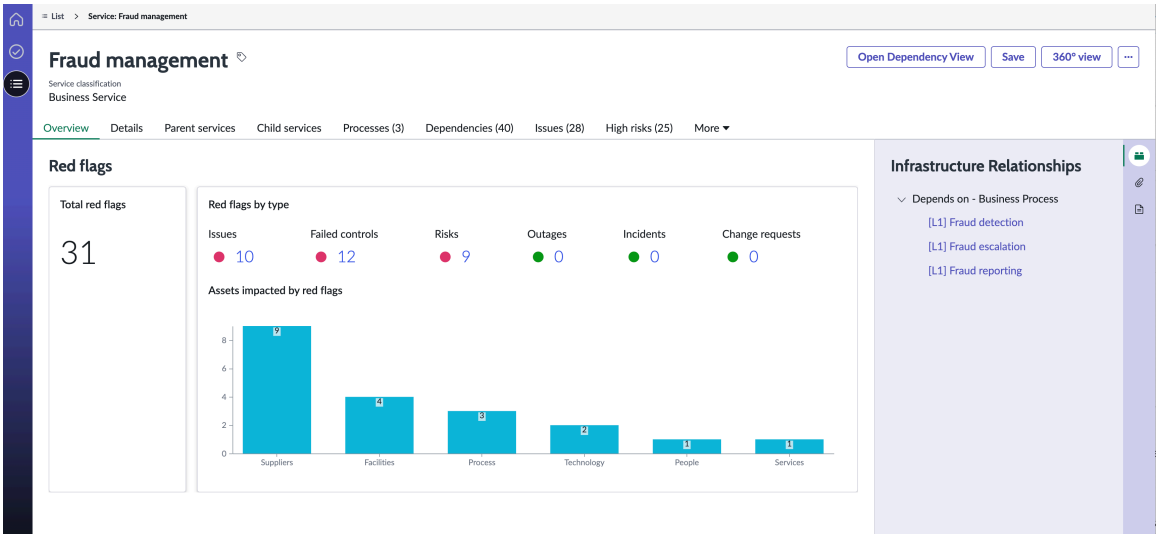



## Overview and Details tabs in the Service form

On the **Overview** tab in the Service form, you can view the resilience metrics for a business service as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

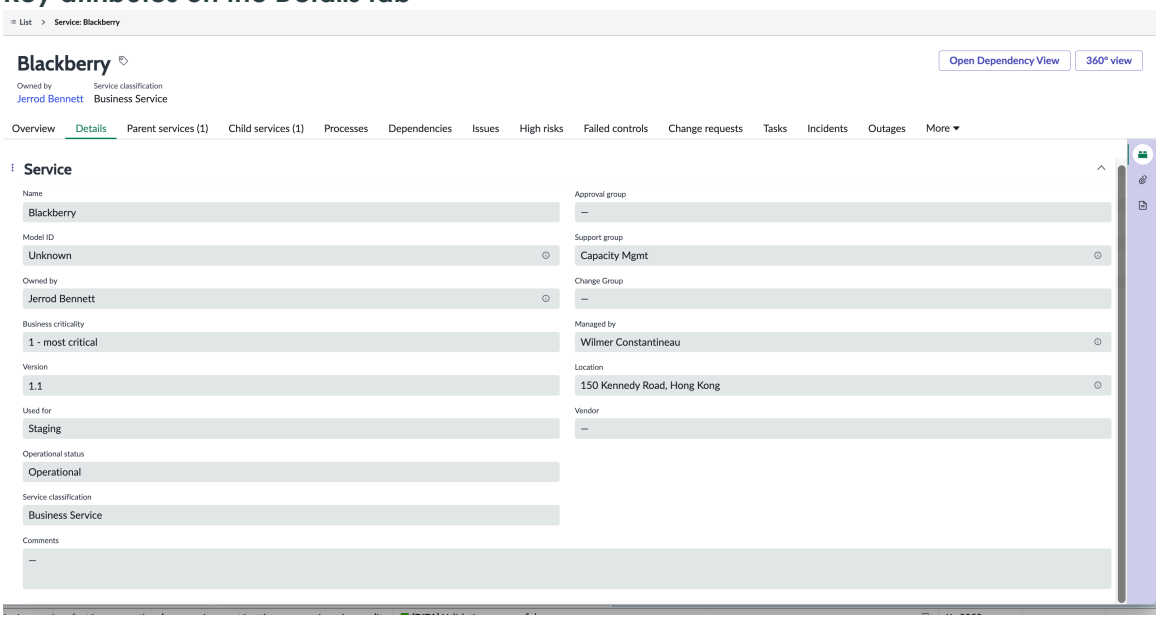
### Resilience metrics on the Overview tab




The Red flags section displays the total number of red flags, red flags by type, and details of the assets that are impacted by the red flags.

On the **Details** tab in the Service form, you can view the key attributes of a business service as shown in the following example:

### Key attributes on the Details tab




## Other related tabs in the Service form

See the following table for more information on the other related tabs in the Service form and their descriptions.

### Other related tabs that are displayed in the Service form

| Tab | Description | New action | Add action | Remove action |
|---|---|---|---|---|
| Parent services | List of the parent services for a business service. To associate an | Form where you can add a parent service. | Table view where you can select multiple | Form where you can remove a parent service |

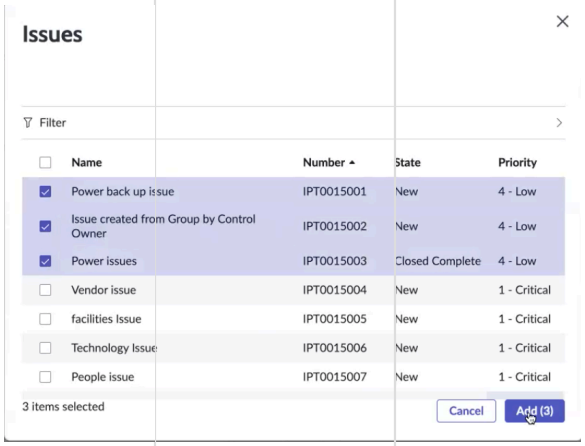
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Other related tabs that are displayed in the Service form (continued)**

| Tab | Description | New action | Add action | Remove action |
|---|---|---|---|---|
| | existing parent service with a business service, select **Add**. To create a parent service for a business service, select **New**. | On this form, you can create a relationship between the parent service and the current service. | services and add them as the parent services of the current service. | from the business service. |
| Child services | List of the child services for a business service . To associate an existing child service with a business service, select **Add**. To create a child service for the current service, select **New**. | Form where you can add a child service. On this form, you can create a relationship between the child service and the current service. | Table view where you can select multiple services that you can add as the child services of the current service. | Form where you can remove a child service from the business service. |
| Processes | List of the processes that are associated with a business service. | Not applicable | Table view where you can select multiple processes that you can add as the child services of the current service. | Form where you can remove a process from the business service. |
| Dependencies | List of the dependencies that are associated with a business service. | Not applicable | Table view where you can select multiple assets (entities) that you can add as the downstream entities of the current service. | Form where you can remove an asset from the business service. |
| Issues | List of the issues that are associated with a business service. Starting with the Utah, you can select **Add** to associate an existing issue with a business service as shown in the following example. | Form where you can create an issue for a business service. | Form where you can add an existing issue to a business service. | Not applicable |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Other related tabs that are displayed in the Service form (continued)**

| Tab | Description | New action | Add action | Remove action |
|---|---|---|---|---|
| | **Add an existing issue to a business service**<br>  <br>To create an issue for a business service, you can also select **New**. | | | |
| High risks | List of the high-risk items or the risk assessments in the monitor state that are associated with the business service. | Not applicable | Not applicable | Not applicable |
| Failed controls | List of the failed or common controls where the status of the control is non-compliant and the reliant entity is the business service. | Not applicable | Not applicable | Not applicable |
| Change requests | List of the change requests that are associated with a business service. | Change Request form. When you submit the Change Request form, the application creates a record | Not applicable | Not applicable |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Other related tabs that are displayed in the Service form (continued)**

| Tab | Description | New action | Add action | Remove action |
|---|---|---|---|---|
| | | in the Services table. | | |
| Tasks | List of the tasks that are associated with a business service. | List of the task tables, from where you can select the type of the task that you want to create. When you submit the form, the application creates a record in the Services with the Tasks table. | Not applicable | Not applicable |
| Incidents | List of the incidents that are associated with a business service. | Incident form. When you submit the Incident form, it creates a record in the Services table. | Not applicable | Not applicable |
| Outages | List of the open outages that are associated with a business service. | Outage form. When you submit the form, the application creates a record in the Services table. | Not applicable | Not applicable |
| Importance and impact assessment | List of the approved Importance and impact assessments. | Not applicable | Not applicable | Not applicable |
| Scenario analysis | List of the approved Scenario analyses. | Not applicable | Not applicable | Not applicable |
| Business continuity plans | List of the Business continuity plans that are associated with a business service. | Not applicable | Not applicable | Not applicable |
| Vulnerability response | List of the responses that are associated | Vulnerability response for a business service. | Not applicable | Not applicable |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

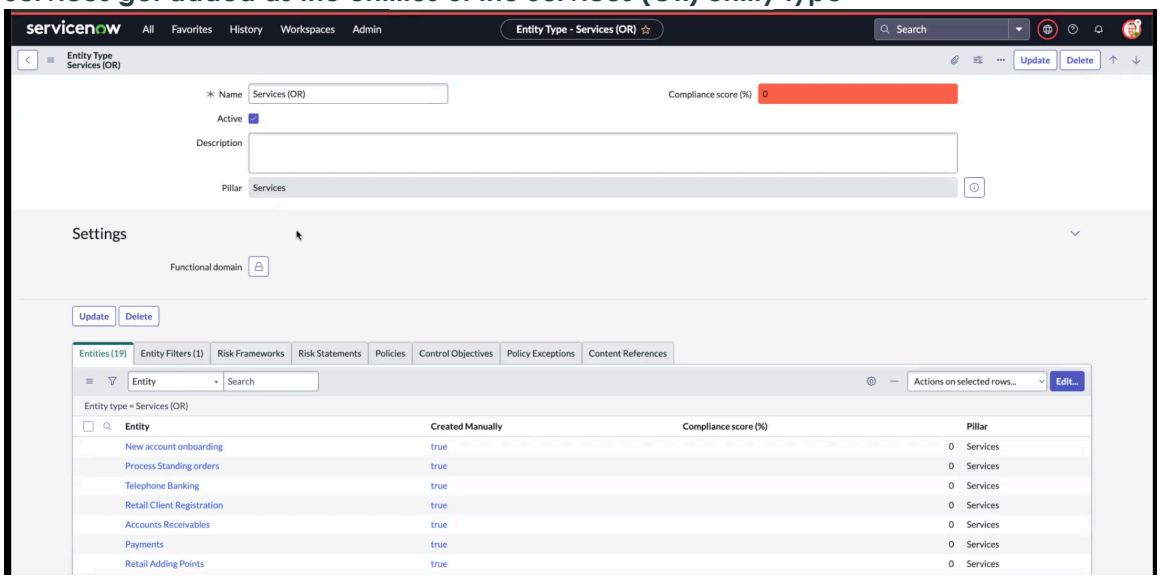
**Other related tabs that are displayed in the Service form (continued)**

| Tab | Description | New action | Add action | Remove action |
|---|---|---|---|---|
| | with a business service. | | | |

## Services as the entities of the Services (OR) entity type

When you add a business service to the Operational Resilience reporting, the service gets added as an entity of the Services (OR) entity type in the Operational Resilience application as shown in the following example.

**Services get added as the entities of the Services (OR) entity type**



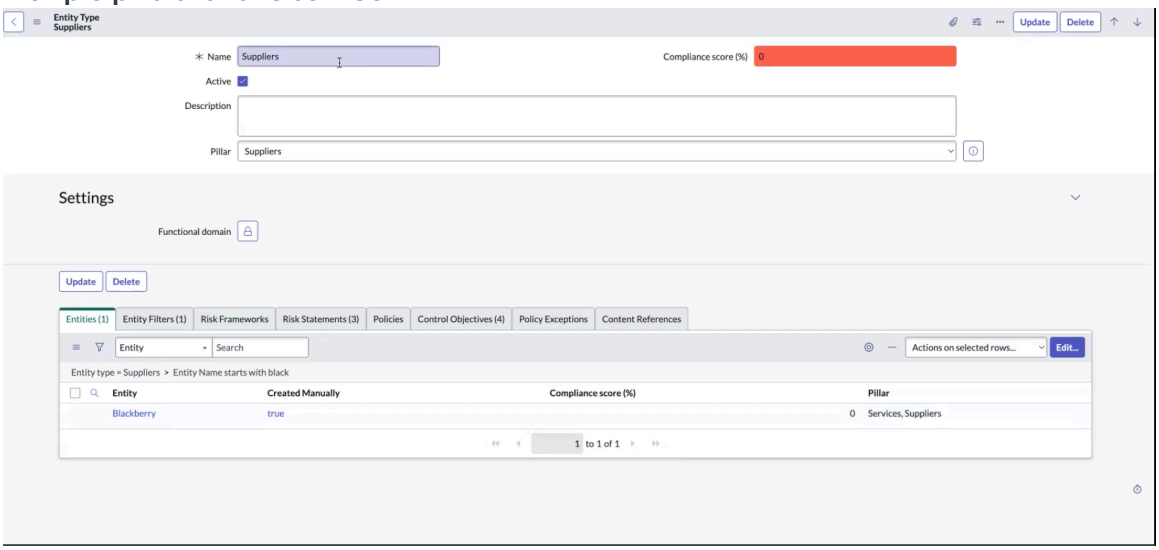

All the services in the Operational Resilience application belong to the Services pillar. As shown in the example, the Pillar column for the entities displays the Services pillar.

**Note:** You can only add the entities that are part of the cmdb_ci_service table to the Services (OR) entity type.

Similarly, in the Operational Resilience application, a service (as an entity) can belong to multiple pillars. The following example shows a service that belongs to two pillars, such as the Services and Suppliers pillars.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

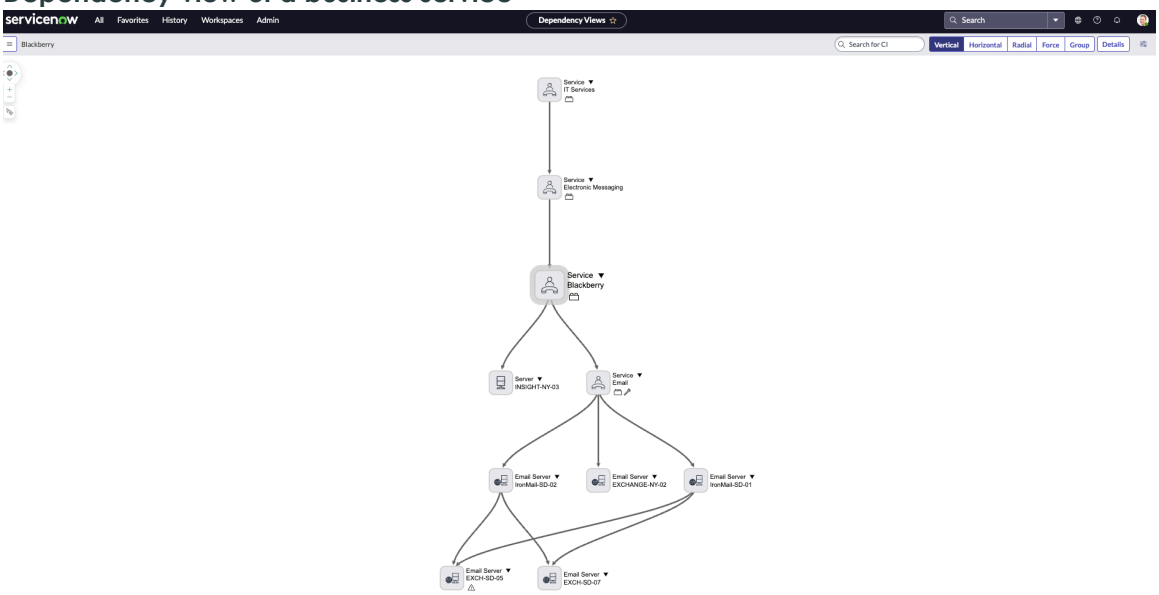
### Multiple pillars for one service




## Open dependency view and 360-degree view for a business service

In the Service form, you can select the **Open dependency view** option to display the infrastructure relationship for a business service. The dependency view of a business service displays its relationship with the parent services, child services, and processes as shown in the following example.

### Dependency view of a business service




On the **360° view** tab, the Operational Resilience managers can monitor the 360-degree view of a service and measure its performance.

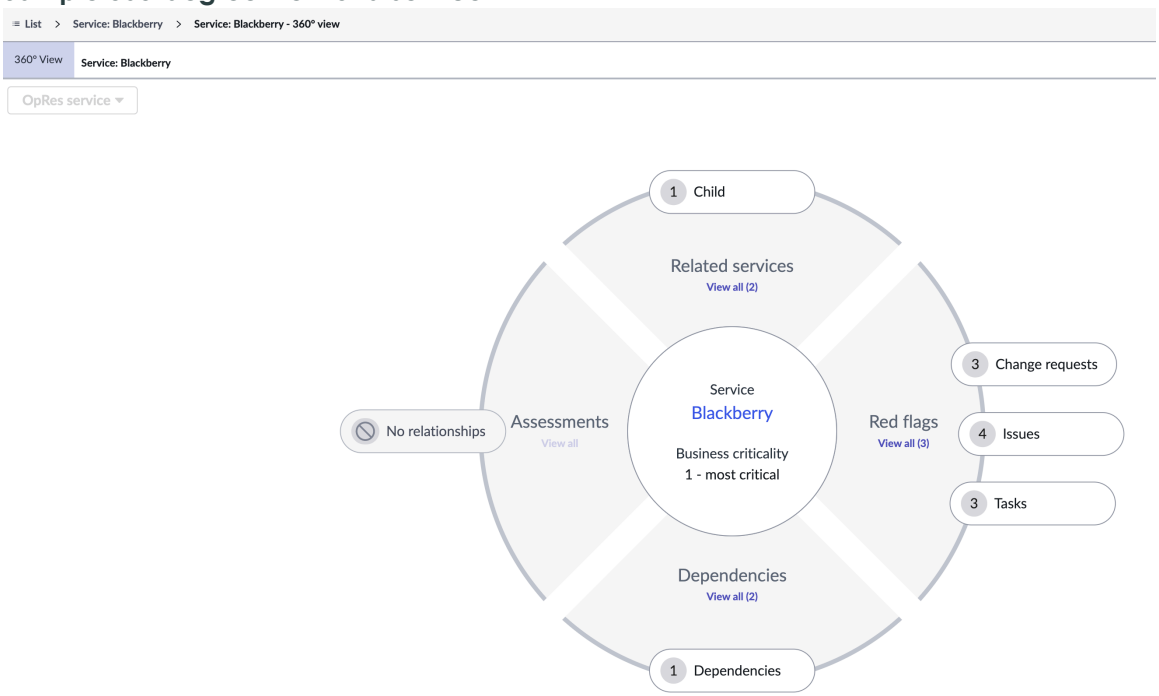
If you have the Operational Resilience manager role, in the 360-degree view for a business service, you can visualize the following entities:

- Parent and child services
- Dependencies that are related to a pillar, such as the Process, Technology, People, Supplier, and Facility pillars in your organization
- Operational Resilience metrics

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following sample 360-degree view displays the relationship of a service with its related entities, such as the red flags, dependencies, and assessments.

**Sample 360-degree view of a service**




For more information on the field values in the Service form, see Create New Service form.

### Add a business service in Operational Resilience Workspace

Add a business service in Operational Resilience Workspace so that you can configure its related tabs, such as the tabs for change requests, incidents, and tasks. You can then view the service attributes and resilience metrics on the dashboard.

## Before you begin

Role required: sn_oper_res.manager with the itil user role, sn_oper_res.admin with the itil user role

## About this task

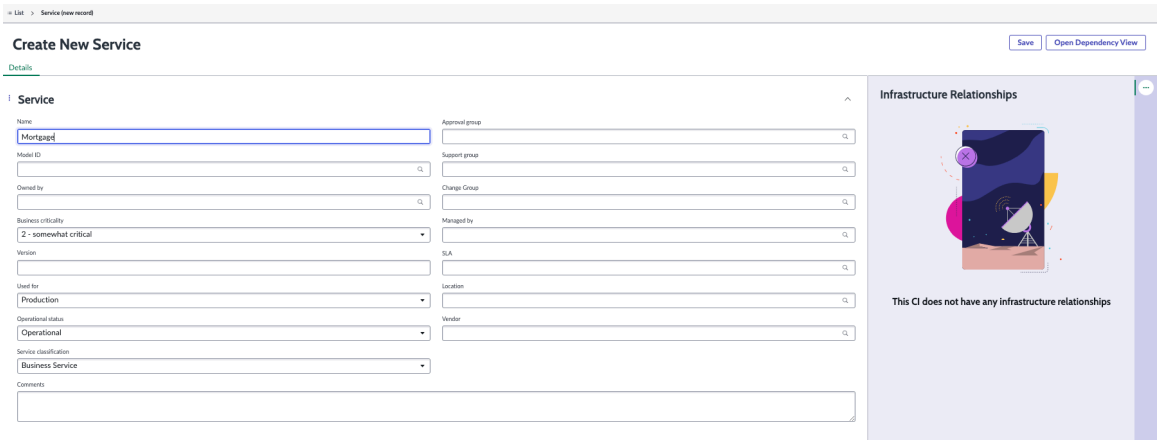
When the *Compute Operational Resilience Compliance* scheduled job runs in the background daily, you can view the status reports of the business services on the Operational Resilience dashboard.

## Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **Services** > **Business Services**.
   A list of the available business services is displayed.
2. Select **New**.
   The Create New Service form is displayed.
3. In the **Details** tab, fill in the fields.
   A sample **Details** tab is shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

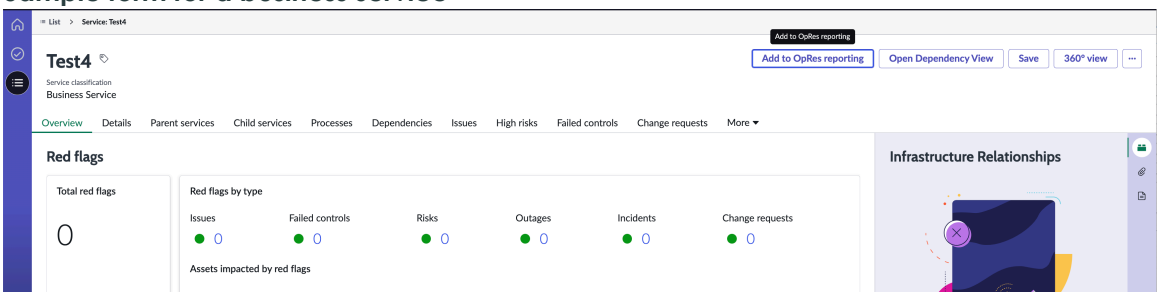
### Details tab in the Create New Service form




For a description of the field values on the Service form, see Create New Service form.

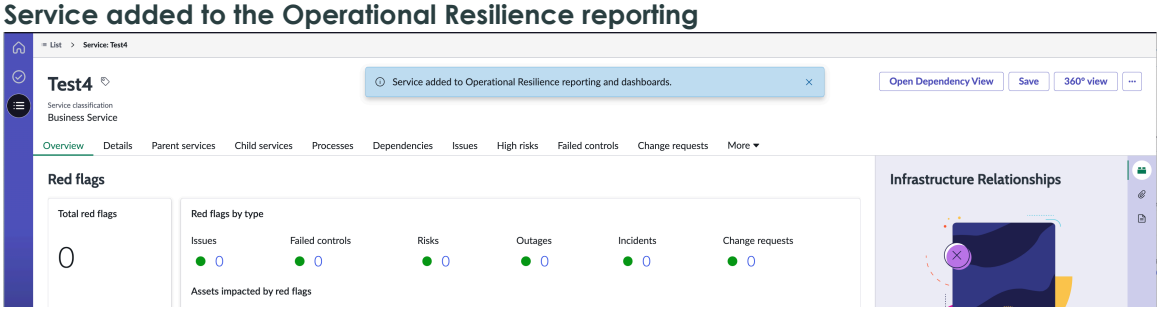
4. To save the details of the service, select **Save**.

### Sample form for a business service




5. To add the business service to the Operational Resilience reporting, select **Add to OpRes reporting**.
   The business service is added to the Operational Resilience reporting and dashboards as shown in the following example.

### Service added to the Operational Resilience reporting

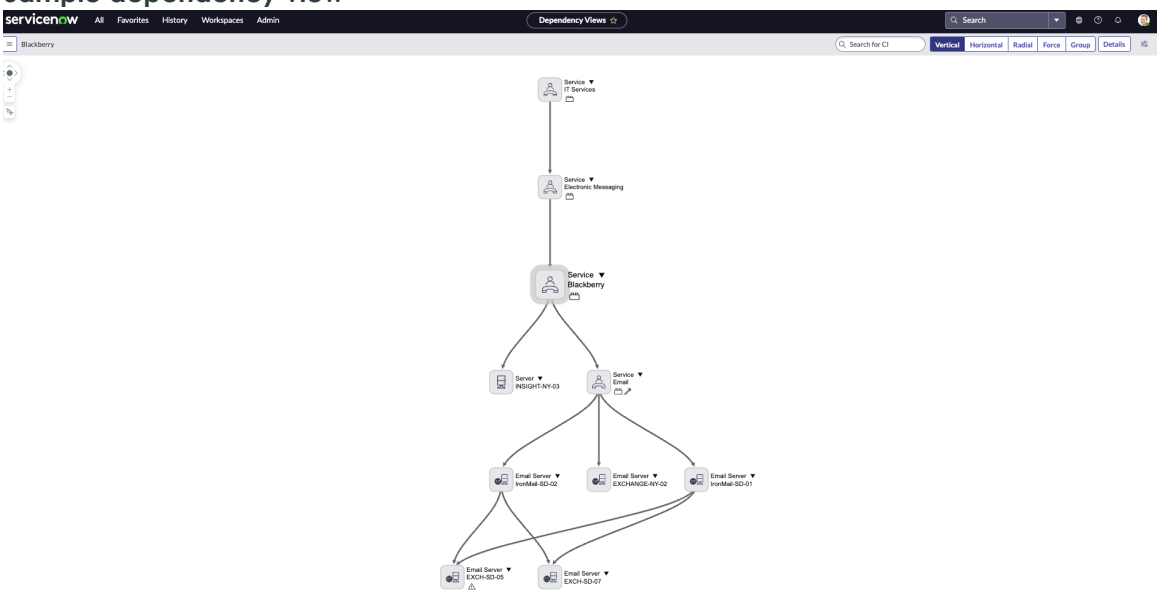



**Note:** After you've added a service to the Operational Resilience reporting, the **Add to OpRes reporting** option isn't displayed for the service anymore on the Service form.

6. To view the infrastructure relationship of the service, select **Open dependency view**.
   The infrastructure relationship of a service with its parent services and child services is displayed as shown in the following example.

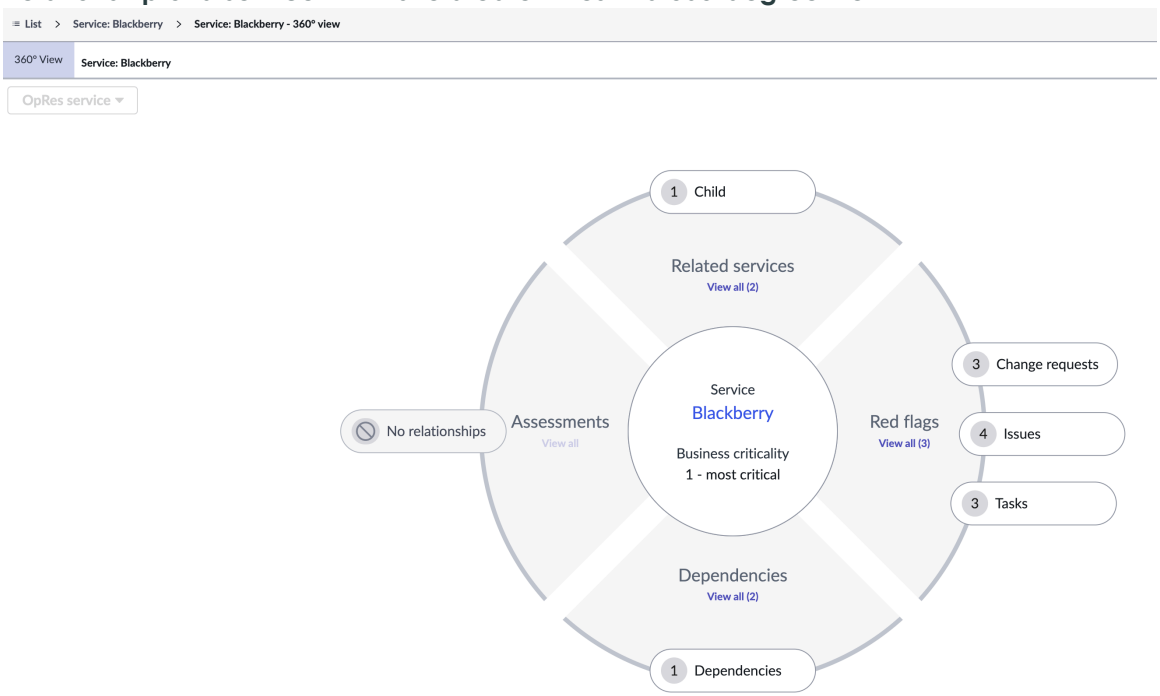
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Sample dependency view




7. To view the relationship of the service with its related entities, select **360° view**.
   The relationship of a service with its related entities, such as the dependencies and red flags in a 360-degree view, is displayed as shown in the following example.

### Relationship of a service with its related entities in a 360-degree view

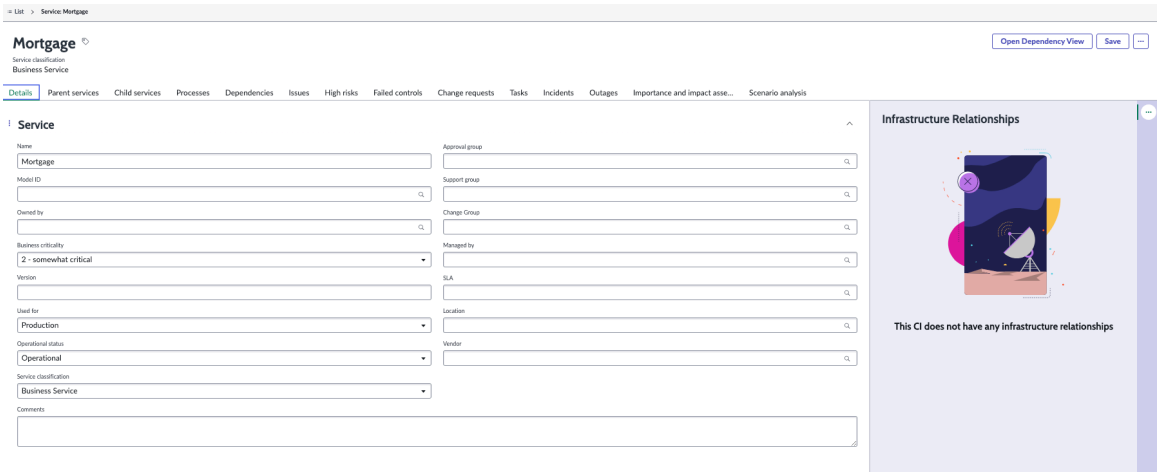



8. To save the details on the form, select **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Service form is displayed as shown in the following example.

**Service form with the related tabs**




## Create New Service form

Use the Create New Service form in Operational Resilience Workspace to set up a business service and configure its related lists.

## Create New Service form

For a description of the field values, see the following table.

### Create New Service form

| Field | Description |
|---|---|
| Overview tab | |
| Importance and impact tolerance assessment | Importance and impact tolerance assessment with the date and timestamp. The tab displays the importance (criticality) of the assessment and the impact tolerance in days. In the form, select **View assessment** to view the Importance and impact tolerance assessment. |
| Details tab | |
| Name | Name of the business service. |
| Approval group | Approval group that is responsible for the approval of the business service. For example, Application Development or Application Security group. |
| Model ID | Model ID for the business service. |
| Support group | Support group for the business service. |
| Owned by | Owner of the business service. This field is auto-filled. |
| Change group | Change group that is responsible for updating the business service. |
| Business criticality | Criticality of the business service. The available options are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Service form (continued)**

| Field | Description |
|---|---|
| | • 1—most critical<br>• 2—somewhat critical<br>• 3—less critical<br>• 4—not critical |
| Managed by | User role that manages the service. |
| Version | Version of the business service. |
| SLA | Service level agreements (SLAs) for the business service. |
| Used for | Usage category that the service is used for. For example, Staging. The available options are as follows:<br>• Production<br>• Staging<br>• QA<br>• Test<br>• Development<br>• Demonstration<br>• Training<br>• Disaster recovery |
| Location | Location of the business service, such as Seattle or Fairfax. |
| Operational status | Operational status of the business service. The available options are as follows:<br>• Operational<br>• Non-Operational<br>• Repair in Progress<br>• DR Standby<br>• Ready<br>• Retired<br>• Pipeline<br>• Catalog |
| Vendor | Vendor that is responsible for operating the business service. |
| Service classification | Classification of the service. The available options are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Service form (continued)**

| Field | Description |
|---|---|
| | • Business Service<br>• Technical Service<br>• Application Service |
| Comments | Comments section for the business service. Typically, the Operational Resilience administrators add the comments about the business service. |

## Related tabs

In the Create New Service form, you can add a parent service, child service, and process for the business service. You can also configure the related tabs, such as the tabs for change requests, incidents, and tasks for the service. You can then view the service attributes and resilience metrics on the dashboard. The following table describes the related tabs that are associated with a service.

**Related tabs that are associated with a service**

| Related tab | Description |
|---|---|
| Parent services | Parent services that are associated with a business service.<br><br>The tab displays the following sample information about the parent services:<br>• Name<br>• Type<br>• Owned by<br>• Managed by<br>• Operational status<br>• Location<br>• Parent |
| Child services | Child services that are associated with a business service.<br><br>The tab displays the following sample information about the child services:<br>• Name<br>• Type<br>• Owned by<br>• Managed by<br>• Operational status |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related tabs that are associated with a service (continued)**

| Related tab | Description |
|---|---|
| | • Location<br>• Child |
| Processes | Processes that are associated with a business service.<br><br>The tab displays the following sample information about the processes:<br>• Name<br>• Owned by<br>• Managed by<br>• Location<br>• Parent |
| Dependencies | Dependencies that are associated with a business service.<br><br>The tab displays the following sample information about the dependencies:<br>• Assets<br>• Pillars<br>• Processes<br>• Child service |
| Issues | Issues that are associated with a business service.<br><br>Beginning with the Utah release, you can add an existing issue with the business service or create an issue related to the business service.<br><br>For the descriptions of the field values on the Create New Issue form, see Create New Issue form. |
| High risks | Details of the high risks that are associated with a business service.<br><br>The tab displays the following sample information about the high risks:<br>• Risk<br>• Risk assessment<br>• Risk statement<br>• Risk response |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related tabs that are associated with a service (continued)**

| Related tab | Description |
|---|---|
| | • Inherent risk<br>• Computed inherent risk<br>• Residual risk<br>• Computed residual risk |
| Failed controls | Details of the failed or common controls that are associated with a business service.<br><br>The tab displays the following sample information about the failed controls:<br>• Control<br>• Control objective<br>• Status<br>• Asset<br>• Pillar<br>• Process<br>• Child service |
| Change requests | Change requests that are associated with a business service.<br><br>The tab displays the following sample information about the change requests:<br>• Change request<br>• Short description<br>• Type<br>• State<br>• Planned start date<br>• Planned end date<br>• Assigned to<br>• Asset<br>• Pillar<br>• Process |
| Tasks | Tasks that are associated with a business service.<br><br>The tab displays the following sample information about the tasks:<br>• Short description<br>• Number |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related tabs that are associated with a service (continued)**

| Related tab | Description |
|---|---|
| | • State<br>• Task type<br>• Priority<br>• Assigned to<br>• Asset<br>• Pillar<br>• Process<br>• Child service |
| Incidents | Incidents that are associated with a business service.<br><br>The tab displays the following sample information about the incidents:<br>• Incident<br>• Short description<br>• Owner<br>• Opened<br>• Caller<br>• Priority<br>• State<br>• Category<br>• Assignment group<br>• Assigned to<br>• Updated<br>• Updated by<br>• Asset<br>• Pillar |
| Outages | Outages that are associated with the current service. You can create an outage for the service.<br><br>The tab displays the following sample information about the outages:<br>• Outage<br>• Type<br>• Begin<br>• End<br>• Asset |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related tabs that are associated with a service (continued)**

| Related tab | Description |
|---|---|
| | • Pillar<br>• Process<br>• Child service |
| Importance and impact assessment | Importance and impact assessment that is done for the service.<br><br>The tab displays the following sample information about the assessment:<br>• Name<br>• Importance<br>• Impact tolerance<br>• Owner<br>• Approver<br>• Updated |
| Scenario analysis | Scenario analysis that is associated with a business service.<br><br>The tab displays the following sample information about the scenario analysis:<br>• Name<br>• Owner<br>• Analysis approver<br>• Updated |
| Business continuity plans | List of the Business continuity plans that are associated with a business service. |
| Vulnerability response | Details of the responses that are associated with a business service. |
| Infrastructure relationships | Infrastructure relationships panel that shows the dependency view for a business service. For example, you can view the servers and services that are associated with a business service in the dependency view. |

## Fetching the dependencies from CMDB and business impact analysis

You can fetch the dependencies for the business services, child services, processes, and processes of the child service from CMDB in Operational Resilience. Similarly, when the BCM applications are installed, the Operational Resilience scheduled job also monitors for the changes in the business impact analysis (BIA) dependencies and fetches the dependency updates.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Fetching the dependencies from CMDB

Beginning with the Utah release, the Data Relationships Framework supports the Operational Resilience application with the underlying framework to fetch the dependencies from CMDB. The Data Relationships Framework (app-grc-relationship-config) is installed with the Operational Resilience application by default. The CMDB dependencies are retrieved by calling an API from the Data Relationships Framework.

To get the CMDB dependencies, the Operational Resilience administrator must activate the main node configuration, labeled as **Business Service (CMDB)** in the Data Relationships Framework first.

For each retrieved dependency, the Operational Resilience application searches for an existing entity first. If there is no existing entity, the dependency is skipped. If there is an existing entity and the entity belongs to any entity type in Operational Resilience, it is added to the downstream of its parent's entity. If the entity does not belong to any entity type, such as Facilities/People/Suppliers/Technology, you must add it manually to the corresponding entity type in Operational Resilience.

The following example shows a sample CMDB relationship setup for a business service. When the service *Windows mobile* updates its dependencies, the entity of *OWA-SD-01* gets added to the downstream of its entity, *IronMail-SD-01* and *IronMail-SD-02* gets added to the downstream of the *Email* child service entity.

**Sample relationship setup for a business service**

| Business service | Associated dependency, business process, and business service: Email | Process and dependencies associated with business service: Email |
|---|---|---|
| Windows mobile | • Dependency: *OWA-SD-01*<br>• Business process: *Inbound payment validation*<br>• Business service: *Email* | • Process: *Fraud_escalation*<br>• Dependency 1: *IronMail-SD-01* (The table is cmdb_ci_email_server.)<br>• Dependency 2: *IronMail-SD-02* (The table is cmdb_ci_email_server.) |

## Fetching the dependencies from the business impact analysis (BIA)

When the BCM applications are installed, Operational Resilience fetches the BIA's dependency update if the BIA's **Applies to** field is a business process used in Operational Resilience.

The following conditions must be met for pulling the BIA dependencies in Operational Resilience:

- The BIA has to be in the **Approved** state.
- The BIA should not be in the **Expired** state.
- The dependency group has to be completed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** Only when the **Applies to** field of the BIA record matches with any business process within the **Business Processes** Entity Type, its dependencies are fetched by the scheduled job.

For each fetched dependency, the Operational Resilience application looks for an existing valid entity first. If the dependency has an existing valid entity and the entity belongs to any entity type in Operational Resilience, it is added to the downstream of its parent's entity.

To fetch the CMDB dependency updates or BIA dependency updates, the following conditions are followed:

- If there is no entity for the dependency, it is skipped. Operational Resilience does not create an entity for the dependency.
- If a dependency entity is inactive, it is ignored.
- If a dependency entity is active, but it has no pillar, it is ignored.
- If a dependency entity is active and has a pillar, but it does not belong to any Operational Resilience entity type, it is ignored.

## Adding the dependencies manually

If the entity does not belong to an entity type such as Facilities, People, Suppliers, Technology, Operational Resilience users must add it to the corresponding entity type manually. Instead of using the scheduled job, Operational Resilience administrators and managers can update the dependencies manually. For information on updating the dependencies manually, see Update the service dependencies manually.

## Support for main node configuration in Data Relationships Framework

For information on the Data Relationships Framework and main node configuration, see Data Relationships Framework and Create a main node configuration record.

### Update the service dependencies manually

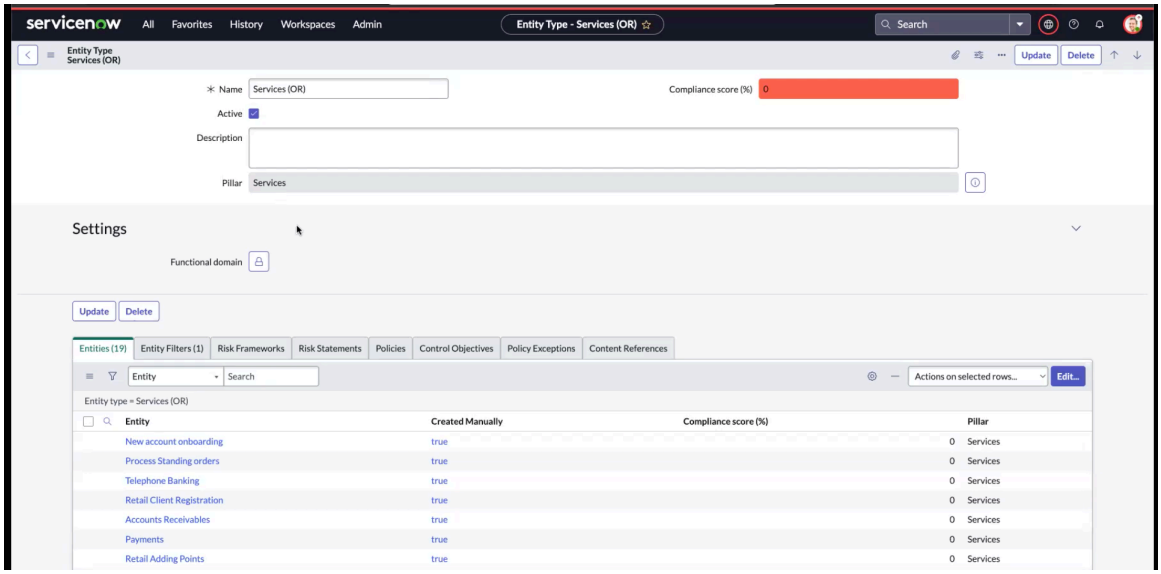
Update the service dependencies manually in the Operational Resilience application.

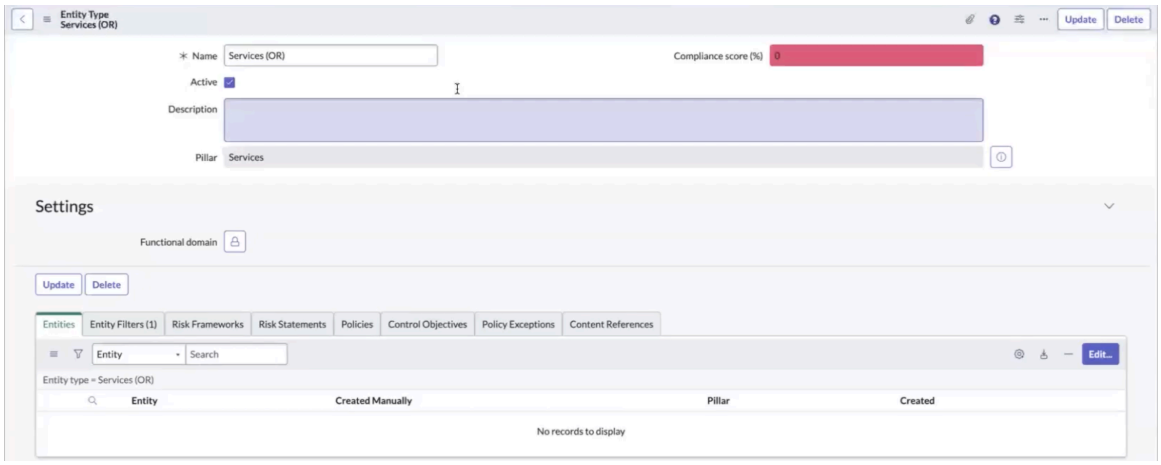
**Before you begin**
Role required: sn_oper_res.admin, sn_oper_res.manager

**Procedure**

1. Navigate to **All** > **Operational Resilience** > **Admin** > **Entity Types**.
2. Select the **Services (OR)** entity type.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**3.** Navigate to the business service record in the Operational Resilience Workspace.

The following example shows the demo data for the Blackberry service where Blackberry is the parent service.

CMDB Relationship Setup

Blackberry

- Email(Child Service)
  - IronMail-SD-01(Dependency)
  - IronMail-SD-02(Dependency)
  - Business process(Business Process)
- Client Management(Business Process)
- INSIGHT-NY-03(Dependency)
- Inbound payment validation(Business Process) // Used to demo the BIA dependency Synch

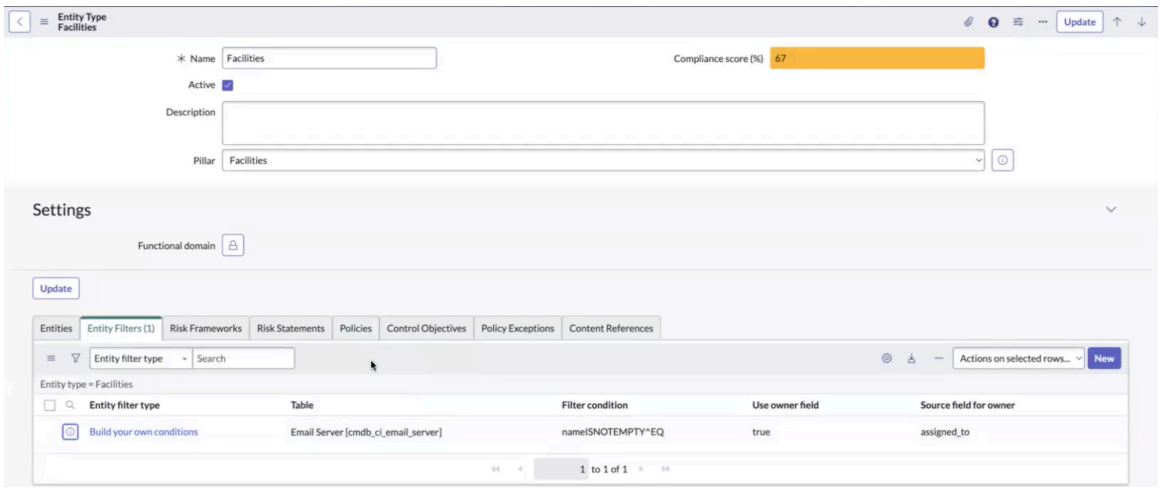
In this example, the parent service has a child service, dependencies, and business processes.

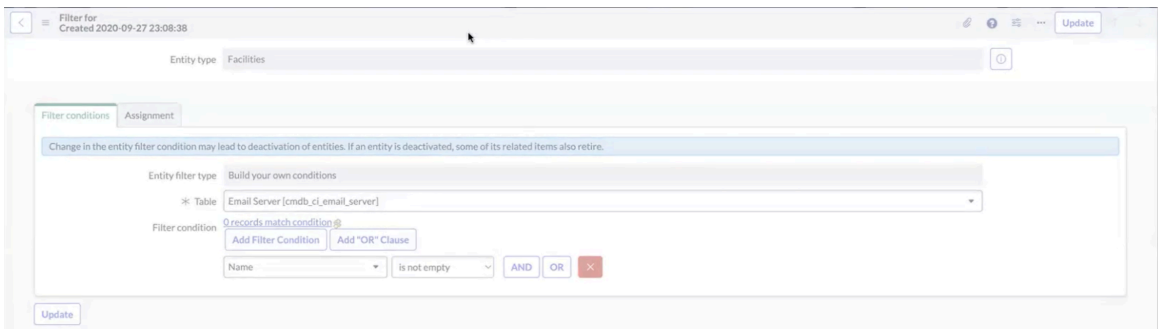
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Email (Child Service)
  - IronMail-SD-01 (Dependency)
  - IronMail-SD-02 (Dependency)
  - Business process (Business Process)
- Client Management (Business Process)
- INSIGHT-NY-03 (Dependency)
- Inbound payment validation (Business Process)

4. Select **Add to OpRes reporting**.
   You can manage the CMDB relationships or monitor the services and processes relationships from the service record in the Operational Resilience Workspace.
   The service is added to the Operational Resilience reporting dashboard. The following message is displayed on the screen: `Service is added to Operational Resilience reporting and dashboards`. The **Add** and **New** action buttons are displayed on the form.
5. To add the entity of a dependency to the entity type by using the filter condition, select the filter condition in **Entity Filters**.

   You can use the filter condition listed in the Entity Filters to add the entities of a dependency as shown in the example.

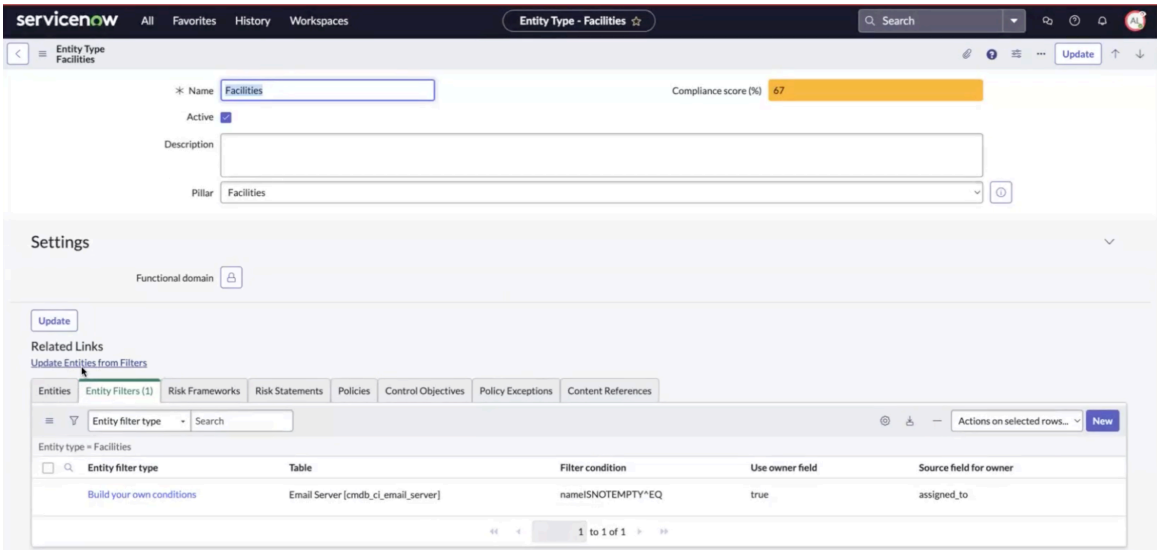



6. Select **Update**.

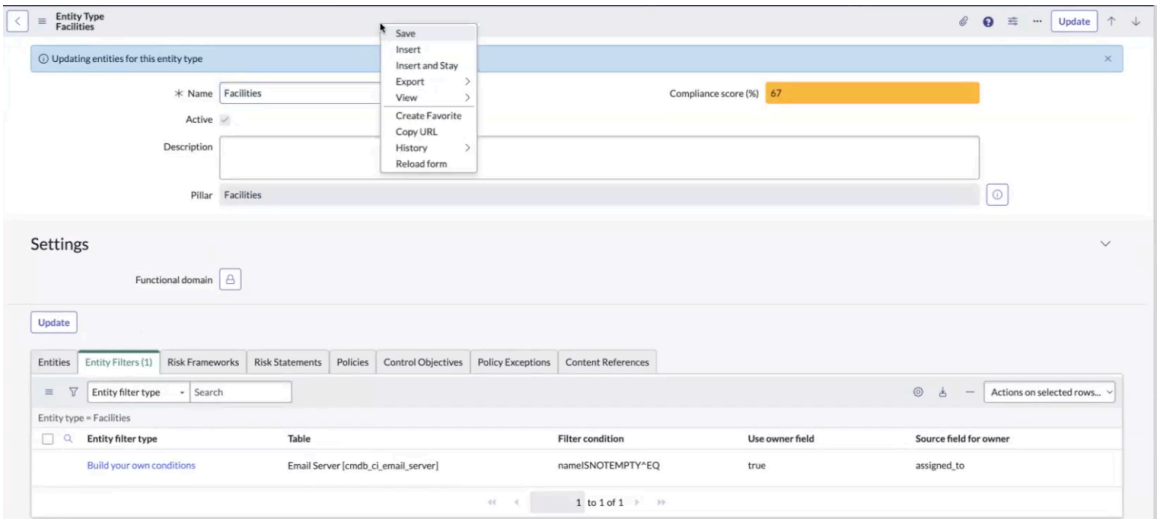
   In Related Links, the Update Entities from Filters link is displayed for updating the entities as shown in the example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



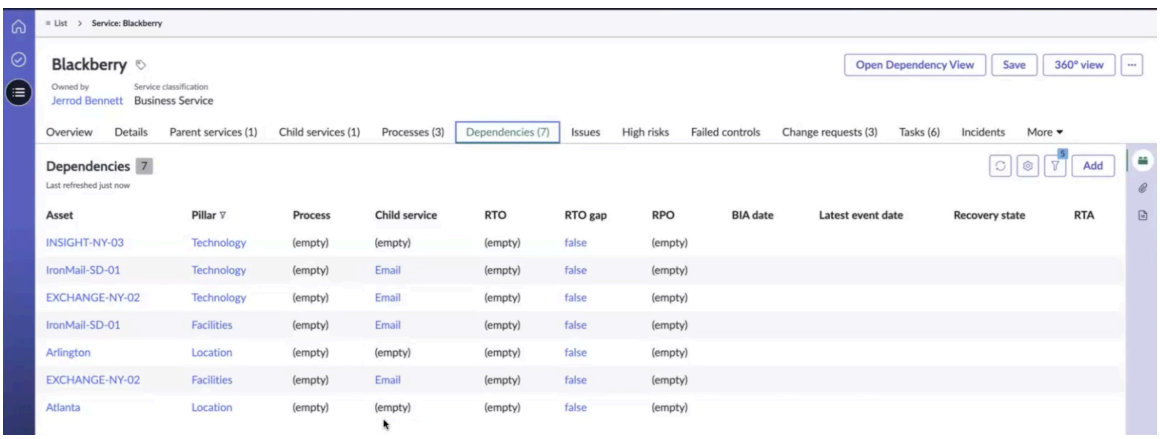

7. Select the **Update Entities from Filters** link.

   The entities are updated for the entity type and the entities are displayed in the Entities related list.




8. To add the dependencies, navigate to the service record and select **Add** in the Dependencies related list.

   The dependencies that are pulled manually are displayed in the list of the service record.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Analyzing the importance and impact tolerance of a business service in Operational Resilience Workspace

By analyzing the importance and the impact tolerance of your business service, you can measure how possible disruptions might impact the performance of a service. You can use the assessment questionnaire template in Operational Resilience Workspace to measure the importance and the impact tolerance of your selected business service.

### Importance and impact tolerance of a business service

A business service's importance is determined by such factors as the number of customers that use the service, the revenue that the service generates, and its impact on your company's brand. By measuring the impact tolerance of a business service, you can see how long a service can be non-operational without causing some kind of loss to the business and its customers.

If you have the sn_oper_res.admin role, you can create and maintain a pre-defined assessment template in Operational Resilience. With the sn_oper_res.manager role, you can select one or more business services that you want to analyze and use the assessment template to calculate the importance and the impact tolerance of your business services.

### Tasks and states that are associated with the assessment workflow

The process for the assessment workflow is as follows:

- The owner of the assessment selects one or more business services and submits the Importance and impact tolerance assessment in Operational Resilience Workspace. This action creates an **Assessment** tab in Operational Resilience Workspace that contains the questions from the pre-populated questionnaire template.
- The assessor of the assessment receives an email notification with a link to the assessment.
- The assessor selects the link for the assessment and responds to the questionnaire. Based on the assessor's responses to the questionnaire, an assessment of the importance rating and the tolerable duration for one or more of the business services is generated.
- After the assessment is completed, the owner reviews the responses and requests an approval for the Importance and impact tolerance assessment. The owner's responses may override the importance and impact tolerance rating of the assessment.
- The approver of the assessment verifies the responses to the questions and approves the assessment.
- The owner of the assessment then closes the assessment in Operational Resilience Workspace.

When you perform the assessment tasks, the assessment is updated through different states in Operational Resilience Workspace as described in the following table.

**States and UI actions that are associated with the assessment**

| State | Associated UI actions | Description |
|---|---|---|
| Draft | Select **New** in the All assessments form. | When you select **New** in the All assessments form, a record is created in the **Draft** state by default.<br><br>Navigate to the **Details** tab and add the assessment |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and UI actions that are associated with the assessment (continued)**

| State | Associated UI actions | Description |
|---|---|---|
| | | details. In the **Services** tab, associate one or more business services with the assessment. |
| Pending response | Select **Assess** in the assessment form. | When you select **Assess** to proceed with the assessment, the application populates the assessment questionnaire under the **Assessment** tab.<br><br>The state of the assessment is then automatically updated to the **Pending response** state. The assessor receives an email notification with a link to the assessment.<br><br>**Note:** To proceed with the assessment, you must associate at least one service with the assessment. |
| Assessment received | Select **Submit** in the assessment template and select **Save** in the assessment form to complete and save the assessment. | When the assessment is in the **Pending response** state, you can respond to the assessment questions that are given in the assessment template. To submit the responses, select **Submit**. To save the assessment, select **Save**. The state of the assessment is updated to **Assessment received**.<br><br>An importance rating and the duration of the impact tolerance are automatically generated based on the questionnaire responses.<br><br>The owner of the assessment requests an approval for the assessment. The approver of the assessment receives an email notification about the assessment. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and UI actions that are associated with the assessment (continued)**

| State | Associated UI actions | Description |
|---|---|---|
| Approved | Select **Request approval** in the assessment form. | The approver of the assessment verifies the responses to the questions and selects **Request approval**. The state of the assessment is automatically updated to **Approved**. |
| Closed | Select **Close** in the assessment form. | An assessment can be closed only when it is in the **Approved** state. To close the assessment, select **Close** in the assessment form. The state of the assessment is updated to **Closed**. |

**Note:** If you have the sn_oper_res.admin role, you can delete the assessment in any state.

If you have the sn_oper_res.admin role, you can set up the assessment ratings by updating the criticality and order of the assessment rating in the Important choices module. For more information on setting up the assessment rating, see Update the assessment rating in the Important choices module.

For more information on the Operational Resilience roles, see Roles installed with Operational Resilience.

### Create an Importance and impact tolerance assessment for a business service

Create an Importance and impact tolerance assessment for a business service in Operational Resilience Workspace. By seeing your customer responses to the questions in the assessment questionnaire, you can measure the importance of your business service and its impact on your customers.

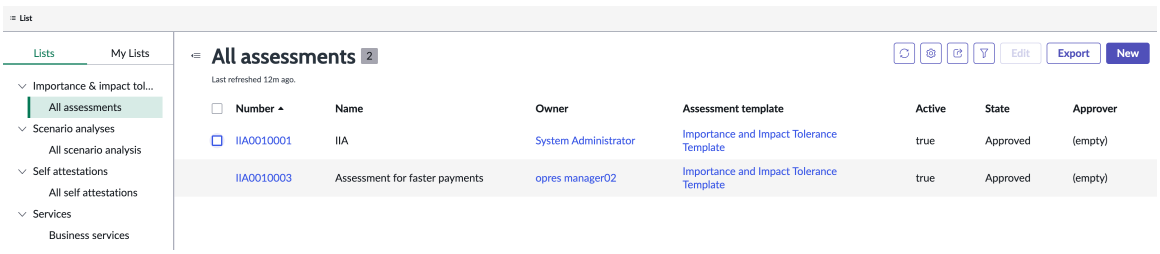
#### Before you begin

Role required: sn_oper_res.user, sn_oper_res.manager

#### Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **List** > **Importance and impact tolerance assessment** > **All assessments**.
   The Importance and impact tolerance assessments in the Operational Resilience application are displayed in the All assessments form as shown in the following example.

**List view in the All assessments form**




2. Select **New**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This action creates an assessment form where you can add the details about the assessment.

3. In the **Name** and **Description** fields, enter the name and description for the assessment.
4. In the **Assessment template** field, select **Importance and Impact Tolerance Template**.
5. In the Assignees panel, select the owner, approver, and assessor for the assessment.

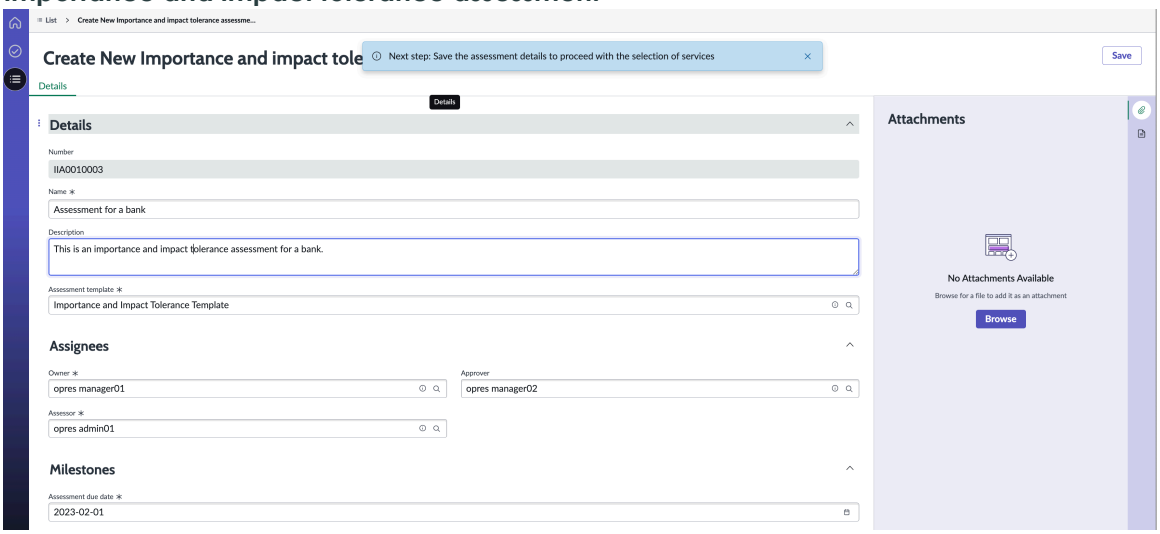
> **Note:** The owner of the assessment can't be its approver.

For a description of the field values on the Importance and impact tolerance assessment form, see Create New Importance and impact tolerance assessment form.

6. In the **Assessment due date** field under the Milestones panel, select the due date for the assessment.
7. Select **Save**.

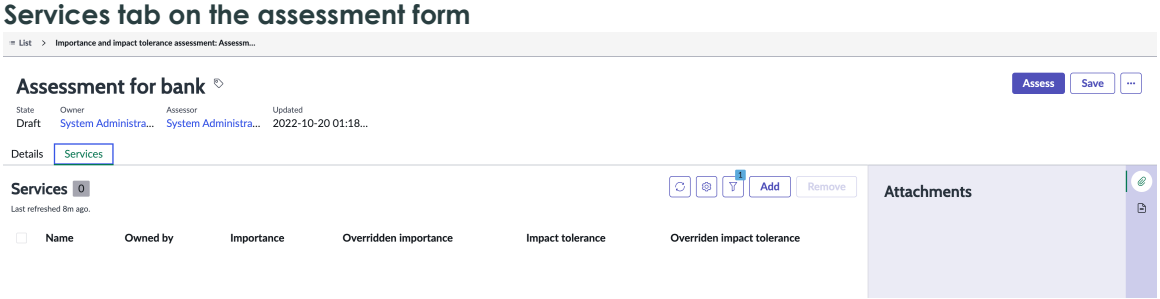
You've created an assessment in the **Draft** state. The details of the assessment are displayed in the assessment form as shown in the following example.

**Importance and impact tolerance assessment**




In the **Services** tab, you can associate a service to the assessment. The **Services** tab is displayed on the assessment form as shown in the following example.

**Services tab on the assessment form**




When the assessment is complete, the **Services** tab displays the information about the associated service, such as its name, owner, importance, overridden importance, impact tolerance, and overridden impact tolerance.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create New Importance and impact tolerance assessment form

Use the Create New Importance and impact tolerance assessment form in Operational Resilience Workspace to create an assessment for your business service.

## Create New Importance and impact tolerance assessment form

For a description of the field values, see the following table.

**Create New Importance and impact tolerance assessment form**

| Field | Description |
|---|---|
| Details panel | |
| Number | Number of the assessment. This field is auto-filled. |
| Name | Name of the assessment. |
| Description | Description of the assessment. |
| Assessment template | Default **Importance and Impact Tolerance Template** field to be filled by the customer. |
| Assignees panel | |
| Owner | Owner of the assessment. This field is auto-filled. |
| Approver | Approver of the assessment. |
| Assessor | Assessor of the assessment. This field is auto-filled. |
| Auto-filled fields that are displayed in the header of the form | |
| State | State of the assessment. This field is auto-filled. |
| Owner | Owner of the assessment. |
| Assessor | Assessor of the assessment. |
| Updated | Time and date to indicate when the details on the form have been updated. |
| Milestones panel | |
| Assessment due date | Date on which the assessment is due. |
| Compose | Private work notes and comments about the assessment. |
| Activity | Details about the activities on the assessment. |

### Add a business service and begin the Importance and impact tolerance assessment

Add a business service to your Importance and impact tolerance assessment. With this assessment, you can get an idea about the impact that possible disruptions can do to your business service.

**Before you begin**

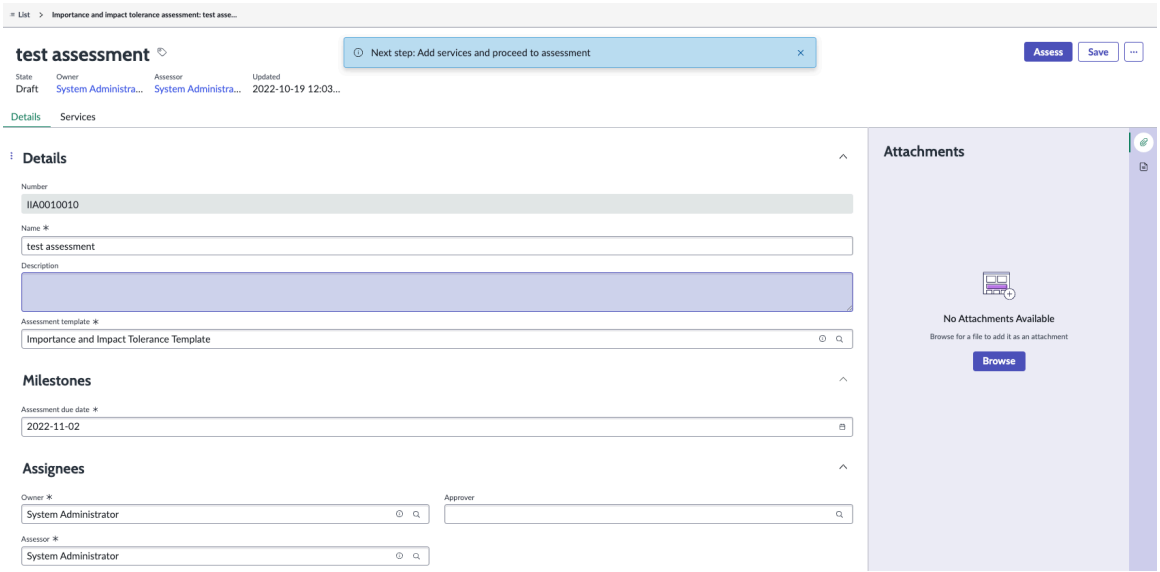
Role required: sn_oper_res.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **List** > **Importance and Impact Tolerance Assessments** > **All Assessments** and select the assessment that you're working on.
   The **Details** tab is updated with the assessment information as shown in the following example.

**Details tab in the assessment form**

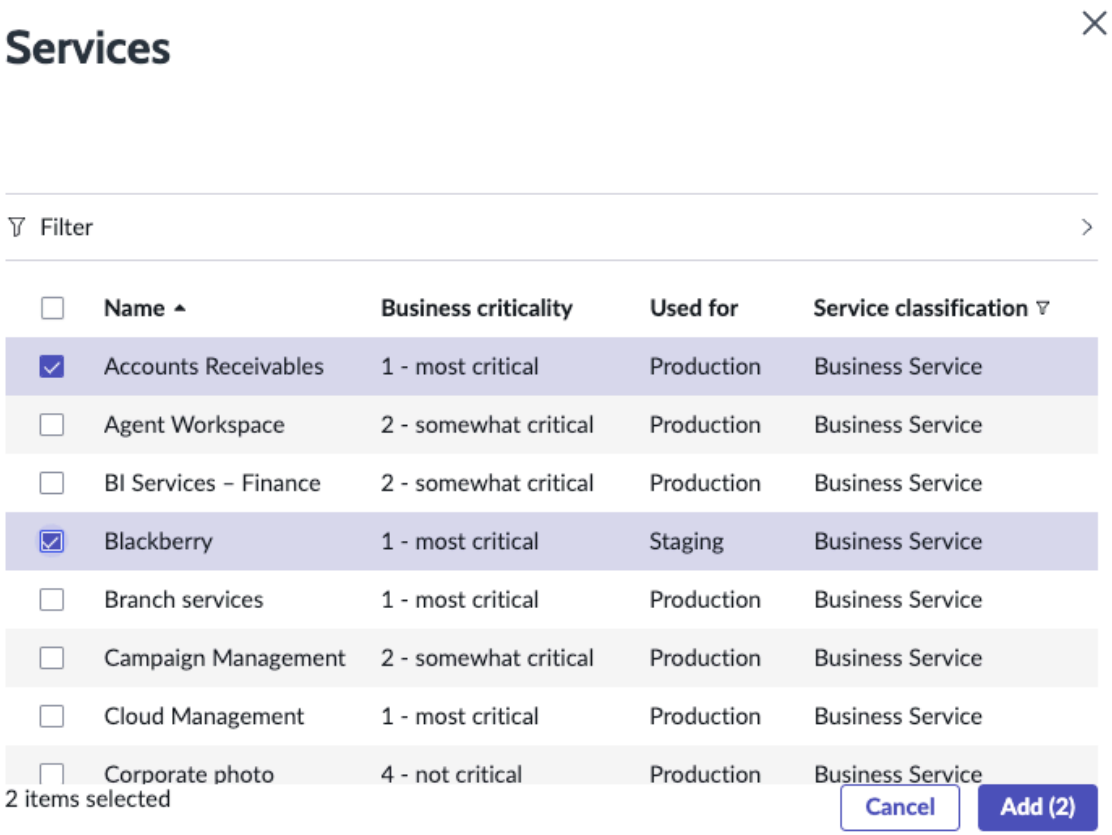



   The **Services** tab is displayed for the assessment.

2. Navigate to the **Services** tab, add services to your assessment, and select **Add**.
   You can add one or more services to the assessment as shown in the following example.

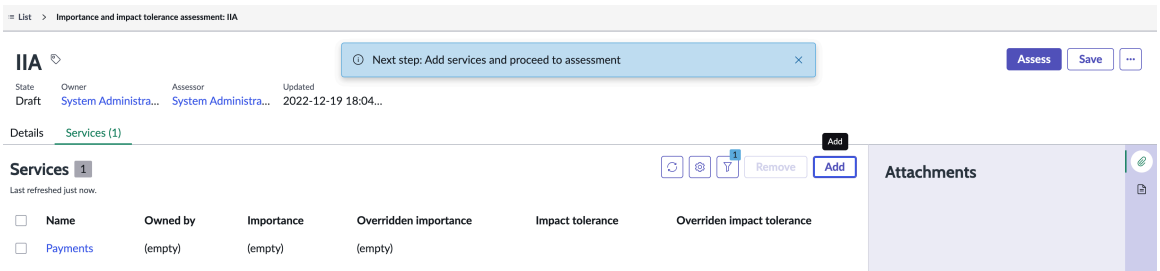
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Add one or more services to the assessment**




In the **Services** tab, the associated services are listed as shown in the following example.

**Services that are associated with the assessment**



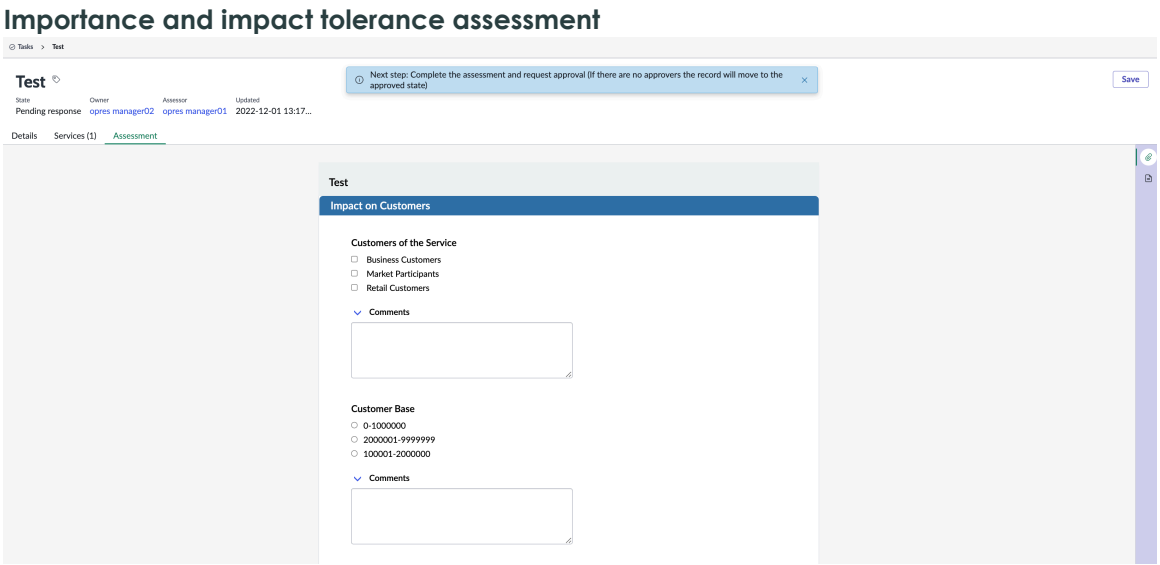

3. Create an assessment by selecting **Assess**.
   When you select **Assess**, an assessment is created in your instance.

   The **Assessment** tab is displayed in the assessment form. The following informational messages are displayed on the screen:

   - *An assessment is created.*
   - *Next step: Complete the assessment and request approval (If there are no approvers, the record will move to the approved state.)*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the **Assessment** tab, the assessment questionnaire is displayed as shown in the following example.




## Result

You've updated the state of the assessment to **Pending response**. The assessor of the assessment receives an email notification with a link to the assessment.

**Note:** If there are no approvers, the state of the assessment automatically changes to the **Approved** state.

### Submit the Importance and impact tolerance assessment for the business service

Log in as an assessor of the Importance and impact tolerance assessment, respond to the questionnaire, and submit the assessment in Operational Resilience Workspace for approval.

## Before you begin

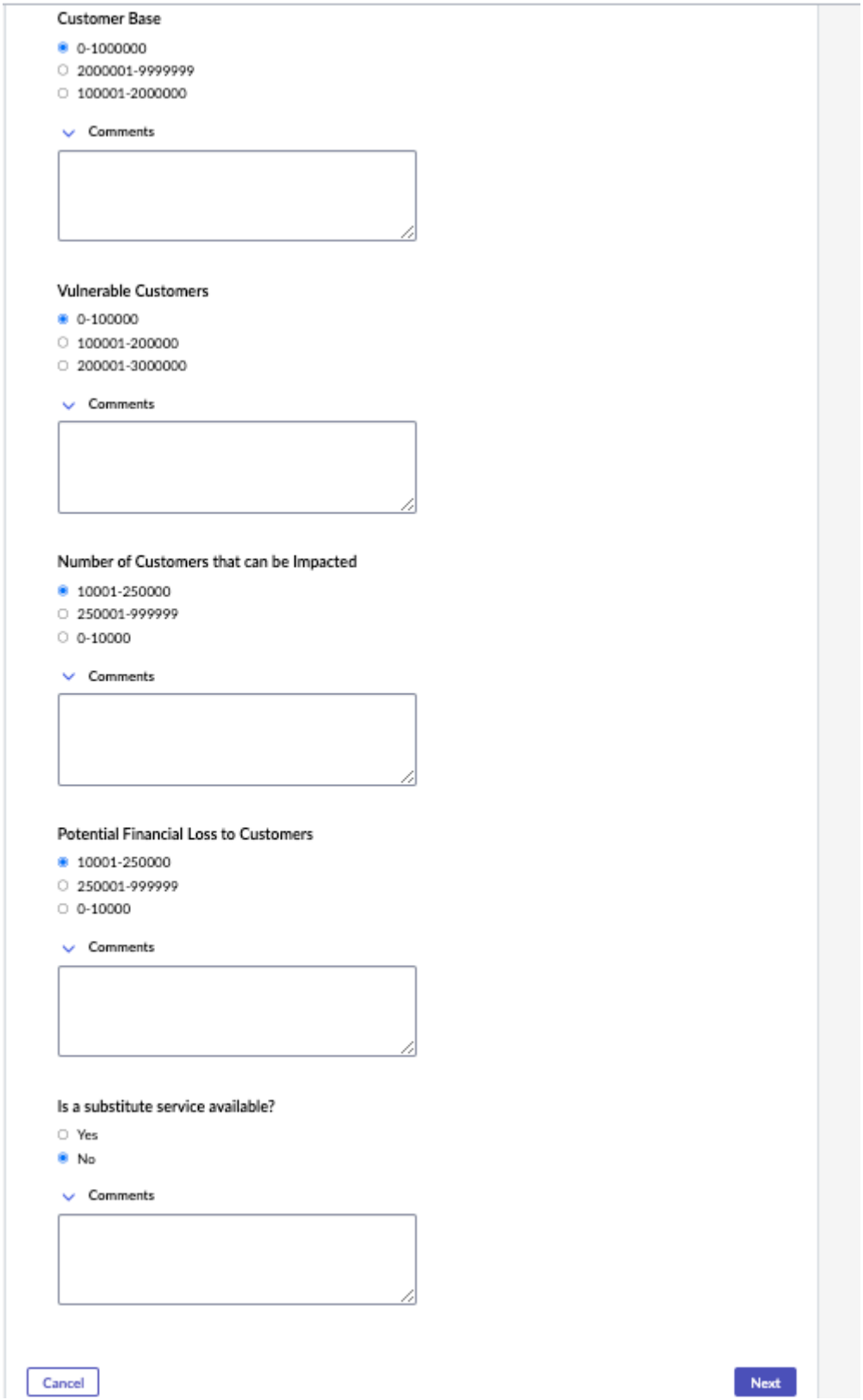
Role required: sn_oper_res.manager

## Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **List** > **Importance and Impact Tolerance Assessments** > **All Assessments** and then to the assessment that you're working on.
2. On the **Assessment** tab, respond to the questions in the assessment.
   As an assessor, you can respond to the questions in the following examples that show the five pages of the Importance and Impact Tolerance Template.

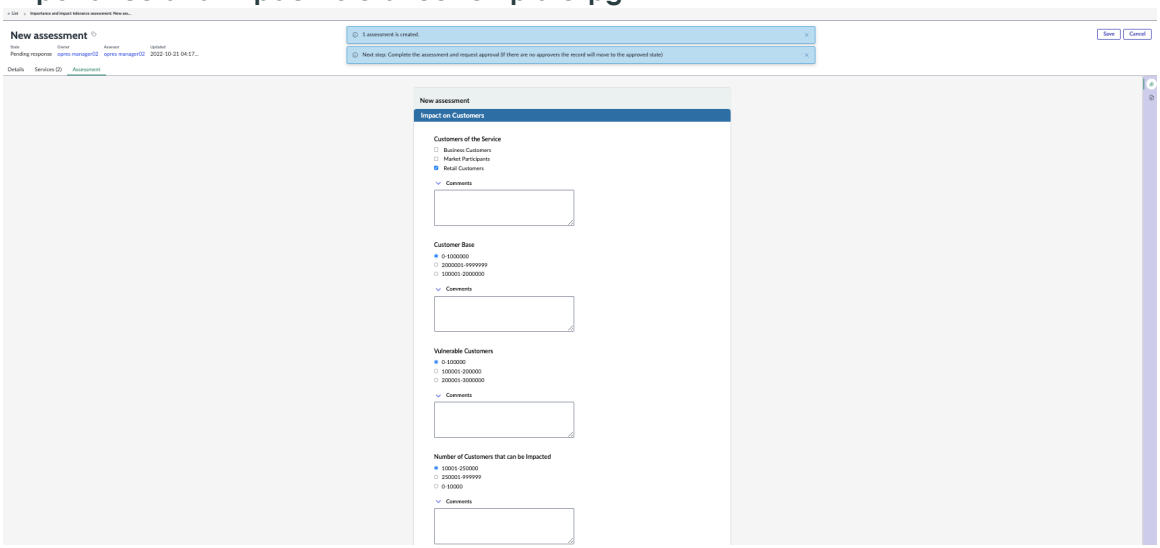
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Importance and Impact Tolerance Template-pg-1

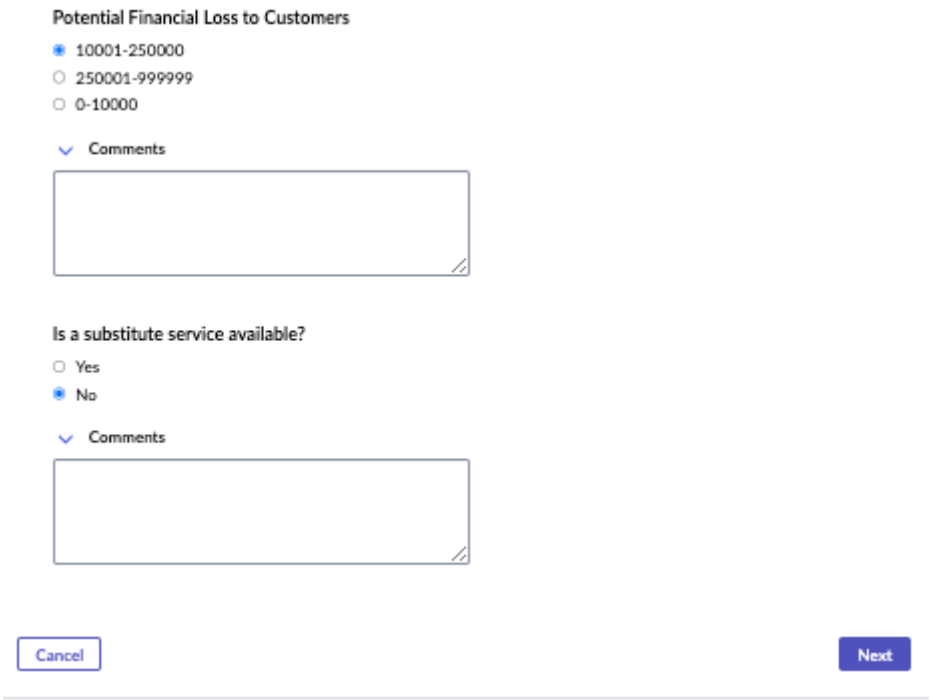



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Importance and Impact Tolerance Template-pg-2

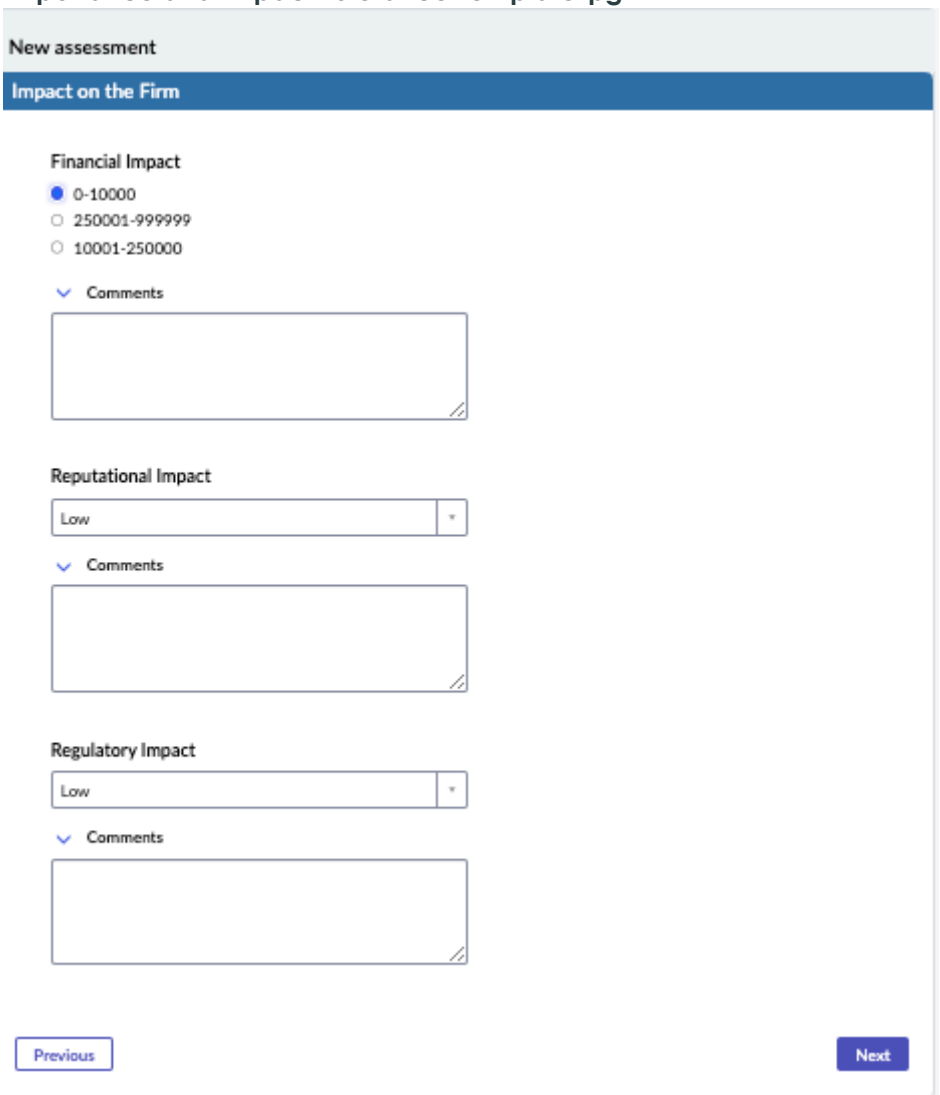



## Importance and Impact Tolerance Template-pg-3

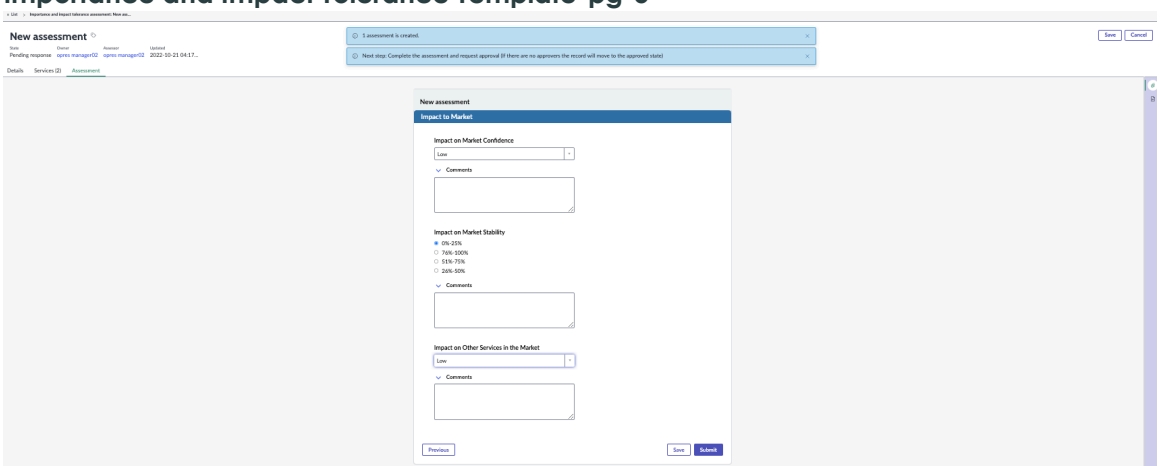



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Importance and Impact Tolerance Template-pg-4




### Importance and Impact Tolerance Template-pg-5




3. In the assessment form, select **Save**.
   After you've answered the required questions, you can save the responses.
4. Select **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

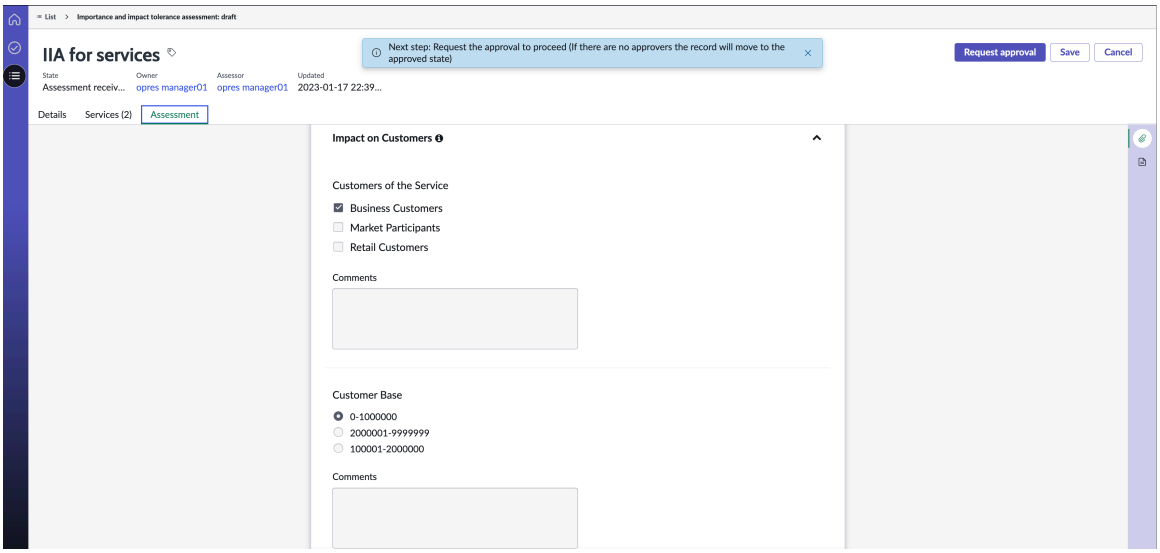
After submitting an assessment, you can track the progress on the assessment in the **Assessment** tab.

When you submit the assessment, the following informational message is displayed on the screen: *Your responses have been submitted. Thanks for taking the Risk Assessment..*

You've updated the state of the assessment to **Assessment received**.

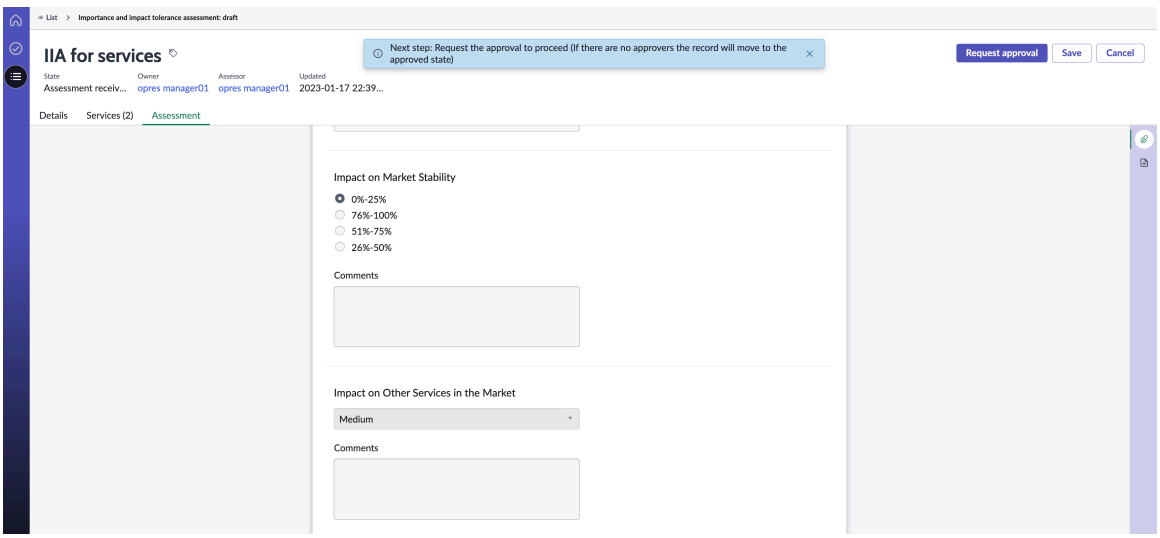
The sample assessment form in the **Assessment received** state is shown in the following example.

**Assessment received**




5. Select **Save**.
   The sample assessment form is shown in the following example.

**Assessment form**




## Request an approval for the Importance and impact tolerance assessment

Request an approval for the Importance and impact tolerance assessment in Operational Resilience Workspace. With an approval, you can make sure that an accurate rating is assigned to your business services.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

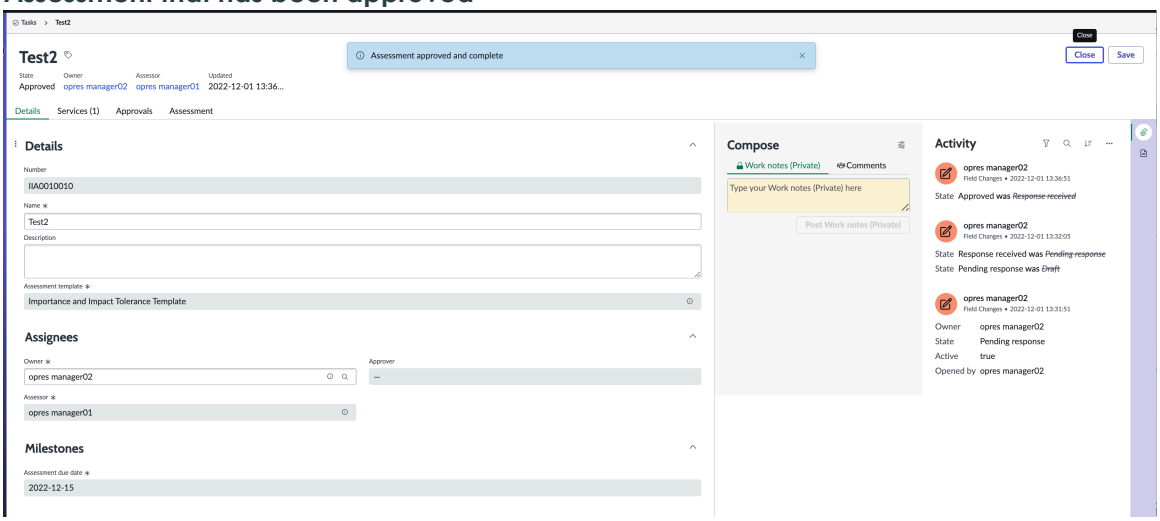
### Before you begin
Role required: sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **Importance and Impact Tolerance Assessments** > **All Assessments** > **Assessment** and then to the assessment that you're working on.
2. Select **Request approval**.

   You've updated the state of the assessment to **Approved**. The *Assessment approved and complete.* message is displayed as shown in the following example.

**Assessment that has been approved**




   The header on the assessment form displays the details on the assessment such as its state, owner, assessor, date, and time that the assessment was updated.

## Close the Importance and impact tolerance assessment

Close the Importance and impact tolerance assessment of a business service so that you can complete the assessment workflow in Operational Resilience Workspace.

### Before you begin
Role required: sn_oper_res.manager

### About this task
After an assessment is approved, a notification is automatically sent to the owner of the assessment that the assessment is approved. The owner of the assessment then closes the assessment.

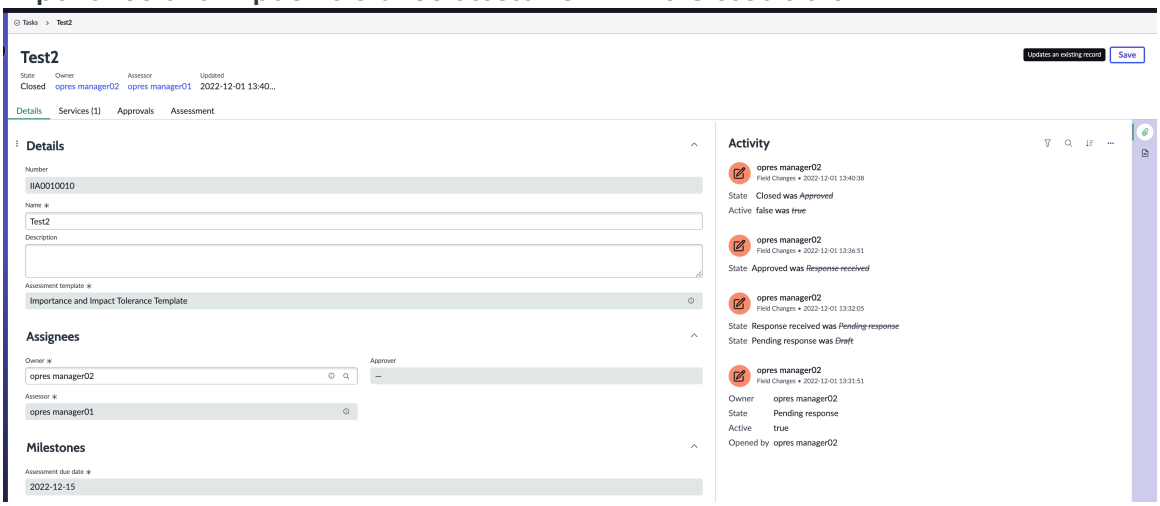
### Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **Importance and Impact Tolerance Assessments** > **All Assessments**.
2. Select the assessment that is in the **Approved** state.
3. Select **Close**.
   By performing this action, you can close the Importance and impact tolerance assessment.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You've updated the state of the assessment to **Closed** as shown in the following example.

**Importance and impact tolerance assessment in the Closed state**




## Performing a scenario analysis in Operational Resilience Workspace

By performing a scenario analysis, you can determine the risks that might impact your business. For example, you can analyze the impact of the scenarios and events on your business services. You can also track the actions and improvements from the scenario analysis in Operational Resilience Workspace.

## Overview of a scenario analysis

Scenarios represent the business-specific risks that are used to test how events can impact your organization. By performing a scenario analysis, you can analyze the impact of the scenarios and their associated events on your business services. Each service has a few dependencies associated with it. The *Compute Operational Resilience Compliance* scheduled job runs in the background and populates the dependencies for the services. As an owner of the scenario analysis, you can request a plan approval.

When a plan approver approves the plan approval, it triggers a response task for the scenario analysis. Participants of the analysis work on the response tasks and add their observations on the analysis.

As an owner of the scenario analysis, you can verify the status of the services and calculate the possible disruptions. After the response tasks have been completed, you can request an analysis approval for your scenario analysis. When an analysis approver approves the scenario analysis, you can close it and monitor its status in Operational Resilience Workspace.

## Tasks to set up a scenario analysis

If you've got the sn_oper_res.manager role, you can set up a scenario analysis as follows:

- Create a scenario that helps you to determine the risks that are applicable to your business.
- Assign an owner, a plan approver, and an analysis approver to the scenario analysis in the scenario analysis form.
- Add the services and dependencies that are applicable to your scenario.
- Associate one or more scenario events with the scenario analysis. Add the participants, services, dependencies, and issues that are specific to a scenario event. When a scenario

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

event is associated with a participant, a response task is automatically generated on the **Responses** tab and it's assigned to the participants.

- Send the scenario analysis to the plan approver of the scenario analysis and request for a plan approval.
- Collect the observations, gaps, and recommendations from the participants about the scenario analysis event. The participants of a scenario event are the users with at least the sn_oper_res.user roles from the associated business functions, such as Finance or HR departments.
- Compare the impact tolerance with the disruption duration to determine if any service was breached.
- Close the open response tasks and open scenario events that are associated with your scenario analysis.
- Send the scenario analysis to the analysis approver for a review and request an approval for the scenario analysis.
- Close the scenario analysis and monitor its status in Operational Resilience Workspace.

## States and UI actions that are associated with a scenario analysis

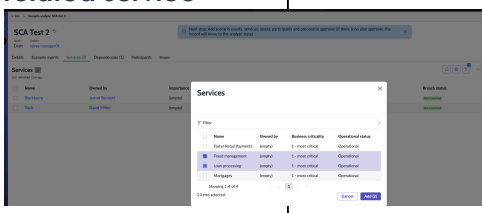
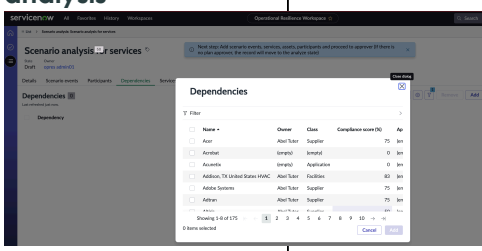
The states and UI actions that are associated with a scenario analysis are described in the following table.

**States and UI actions that are associated with a scenario analysis**

| State | UI action | Description |
|---|---|---|
| Draft | In the All scenario analysis form, select **New**. | More details about the UI actions for this state:<br>• In the All scenario analysis form, select **New**, add information in the **Details** tab, and select **Save**. A record is automatically created in the **Draft** state.<br>• On the **Services** tab, select **Add** to add a service from the list of the available services as shown in the following example.<br>**Add a service to the scenario analysis**<br>  |

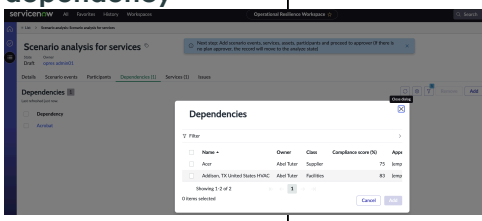
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and UI actions that are associated with a scenario analysis (continued)**

| State | UI action | Description |
|---|---|---|
| | | **Note:** The services are fetched from the Services (OR) entity type in the Operational Resilience application.<br><br>• Some services in the Operational Resilience application are associated with specific dependencies, for example, Acer or Adtran. To select a service that is associated with a dependency, select **Add dependency related service** as shown in the following example.<br><br>**Add dependency related service**<br>  <br><br>• On the **Dependencies** tab, select **Add** to associate a dependency with the scenario analysis as shown in the following example.<br><br>**Add a dependency to a scenario analysis**<br>  |

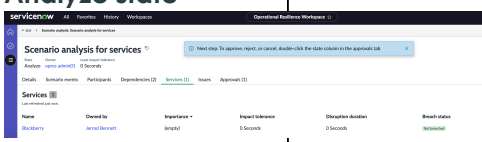
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and UI actions that are associated with a scenario analysis (continued)**

| State | UI action | Description |
|---|---|---|
| | | Some dependencies are associated with specific services. You can add a dependency that is related to a specific service by selecting **Add service related dependency** as shown in the following example.<br>**Add service related dependency**<br>  <br>• To save the selections, select **Save**.<br>• In the scenario analysis form, select **Request plan approval** to request a plan approval from the plan approver of the scenario analysis.<br>**Note:** You must associate at least one service to begin the scenario analysis. |
| Pending plan approval | Navigate to the **Approvals** tab, update the state from **Requested** to **Approved,** and then in scenario analysis form, select **Save**. | More details about the UI actions for this state:<br>• As the plan approver of the analysis, you must review the scope of the analysis in the **Pending plan approval** state. You can check the setup of the associated services, participants, scenario events, and issues.<br>• To approve the plan for the analysis, navigate to the **Approvals** tab, update |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and UI actions that are associated with a scenario analysis (continued)**

| State | UI action | Description |
|---|---|---|
| | | the state from **Requested** to **Approved**, and then in the scenario analysis form, select **Save**.<br><br>• When you approve the plan for the scenario analysis and save it, the state of the scenario analysis is updated to **Analyze**.<br><br>• If you reject the plan, the state of the scenario analysis is reset to **Draft**. |
| Analyze | On the **Scenario events** tab, add a scenario event to the analysis by selecting **Add**. On the **Participants** tab, add a participant to the analysis by selecting **Add**.<br><br>On the **Scenario events** tab, update the state to **Closed** to close the scenario event. Select **Request analysis approval**. | More details about the UI actions for this state:<br><br>• In this state, the participants of the scenario analysis can add their work notes in the scenario analysis form and work on events that are based on their responsibility.<br><br>A sample scenario analysis form is shown in the following example.<br><br>**Tabs in the Analyze state**<br>  <br><br><br>**Note:** You must add at least one service, one participant, and one scenario event before proceeding with the scenario analysis.<br><br>• On the **Scenario events** tab, select **Add** to associate one or more scenario events with the analysis. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and UI actions that are associated with a scenario analysis (continued)**

| State | UI action | Description |
|---|---|---|
| | | • On the **Participants** tab, select **Add** to associate one or more participants with the analysis. When a scenario event is created, a response task is automatically created and assigned to the participant. You can collect the feedback from the participants and review their observations, gaps, and recommendations for each associated event on the form.<br>• Navigate to the **Responses** tab and close the response tasks that are associated with a scenario event.<br>• Update the state of the scenario event from **Draft** to **Completed** and close the open scenario event. Select **Save**.<br>• Based on the observations and recommendations, the details of the scenario analysis are auto-filled in this state in the scenario analysis form. To request an approval from the analysis approver, in the analysis form, select **Request analysis approval**. The state of the scenario analysis is then updated to **Pending analysis approval**. |
| Pending analysis approval | Navigate to the **Approvals** tab and update the state from **Requested** to **Approved**. | If you're the analysis approver, you can review the analysis scope in this state. Check the progress on the analysis for the selected business service. You can |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and UI actions that are associated with a scenario analysis (continued)**

| State | UI action | Description |
|---|---|---|
| | | then approve or reject the analysis. |
| Approved | In the analysis form, select **Save**. | When you approve the scenario analysis, the state of the scenario analysis is updated to **Approved**. If you reject the scenario analysis, the state of the scenario analysis is reset to **Analyze**.<br><br>When the state of the scenario analysis is in the **Approved** state, you can close the scenario analysis. |
| Closed | In the analysis form,select **Close**. | As an owner of the scenario analysis, you can close the scenario analysis. The state is updated to **Closed**. |

## Fetching the service entities from the Services (OR) entity type

The Operational Resilience application fetches the service entities from the Services (OR) entity type as shown in the following example.

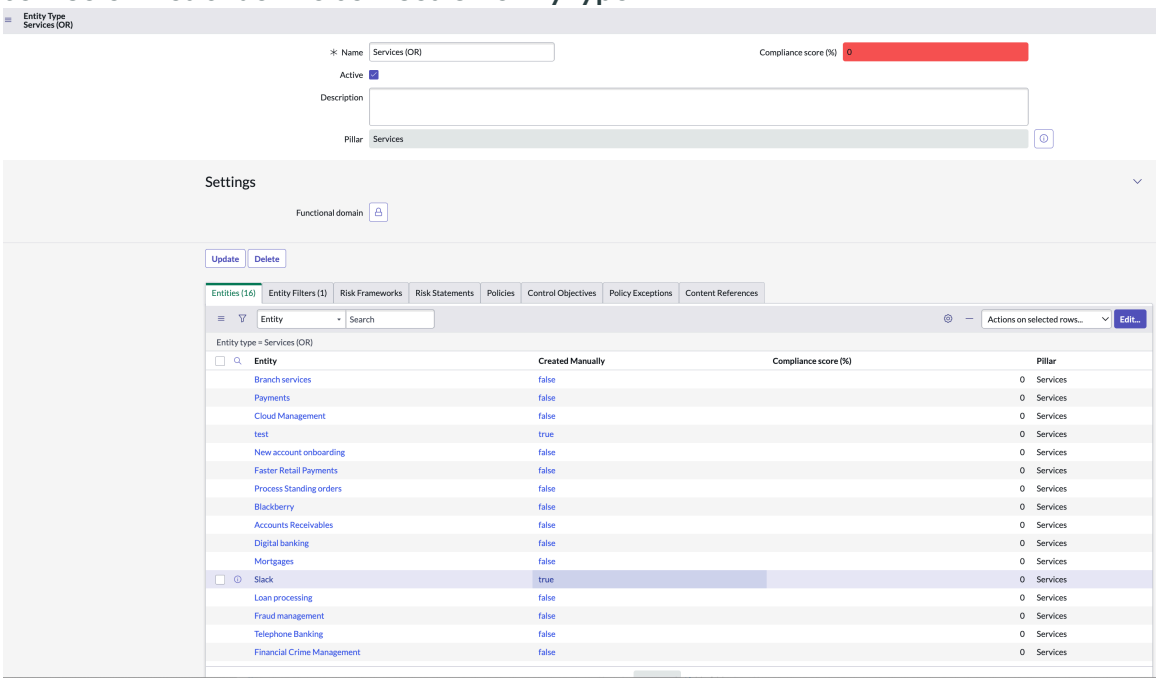
**Services OR entity type**




Users with the sn_oper_res.admin role can view the Entity Types module and its related lists in the Operational Resilience application UI as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Service entities under the Services OR entity type

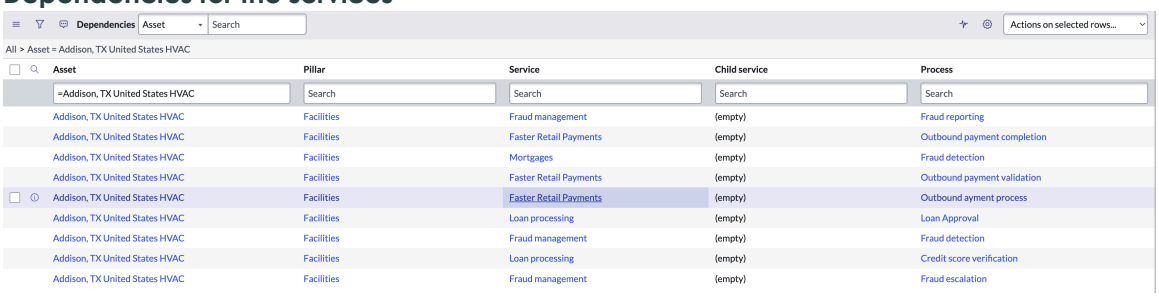



**Note:** You can only select the entities that belong to the Facilities, People, Suppliers, and Technology pillars. The Services and Processes pillars are filtered out from the list of the pillars for the entities.

## Dependencies for the services

Each service has a few dependencies associated with it. The *Compute Operational Resilience Compliance* scheduled job runs in the background and populates the dependencies for the services. The following example shows that the Addison, TX United States HVAC entity is listed as a dependency for supporting the Faster Retail Payments service.

### Dependencies for the services



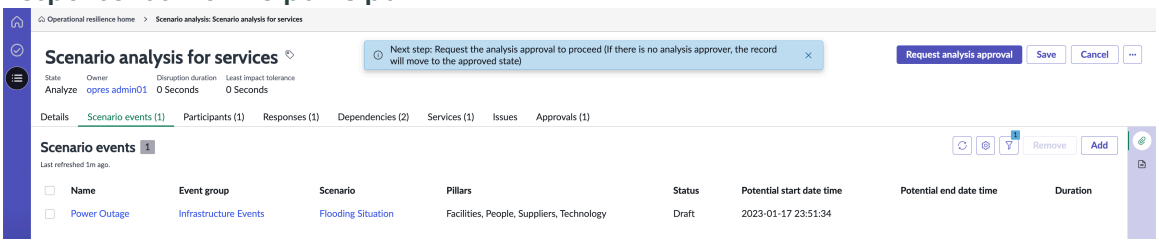

You can only select the dependencies that belong to the Facilities, People, Suppliers, and Technology pillars. The Services and Processes pillars are filtered out from the list of the pillars for the dependencies.

## Response tasks

As a scenario analysis owner, when you create a scenario event and add a participant to it, a response task is automatically created for the participant. The following example shows that when a participant is assigned to a scenario event, a response task is created. An email notification is automatically sent to the participant.

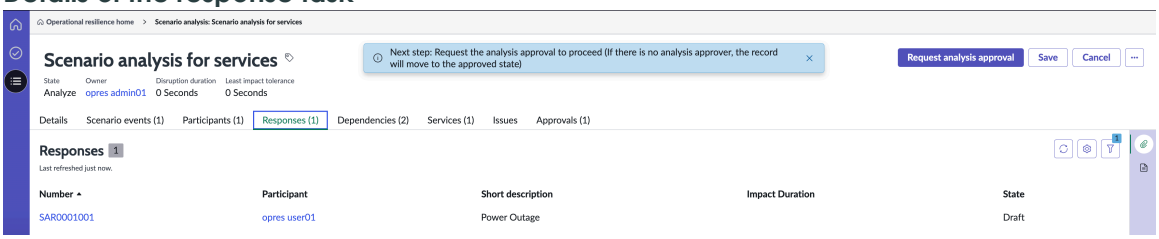
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Response task for the participant



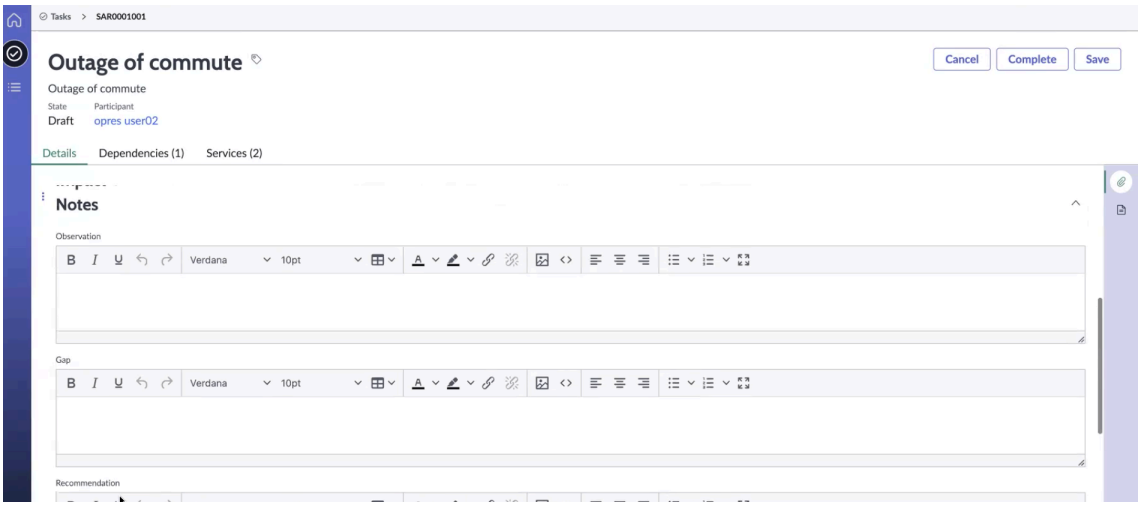

On the **Responses** tab, the details of the response task such as the response task number, name of the assigned participant, and state of the response task are displayed as shown in the following example.

### Details of the response task




The owner of the scenario event can add a service and a dependency to the response task. The assignee of the response task can complete the response task, add their notes about the scenario event, and update the impact duration of the scenario event as shown in the following example.

### Notes about the scenario event




## Known issue for upgrading from Release 15.x.x to Release 16.x.x

While upgrading from Release 15.x.x to Release 16.x.x, if you have a scenario analysis in the **Analyze** state and a participant is already added to the scenario analysis, a response task is not created automatically. This is a known issue.

As a workaround for this issue, the Operational Resilience manager must remove the participants from the scenario analysis and add them to the same scenario analysis. The Operational Resilience application then automatically creates a response task for the scenario analysis.

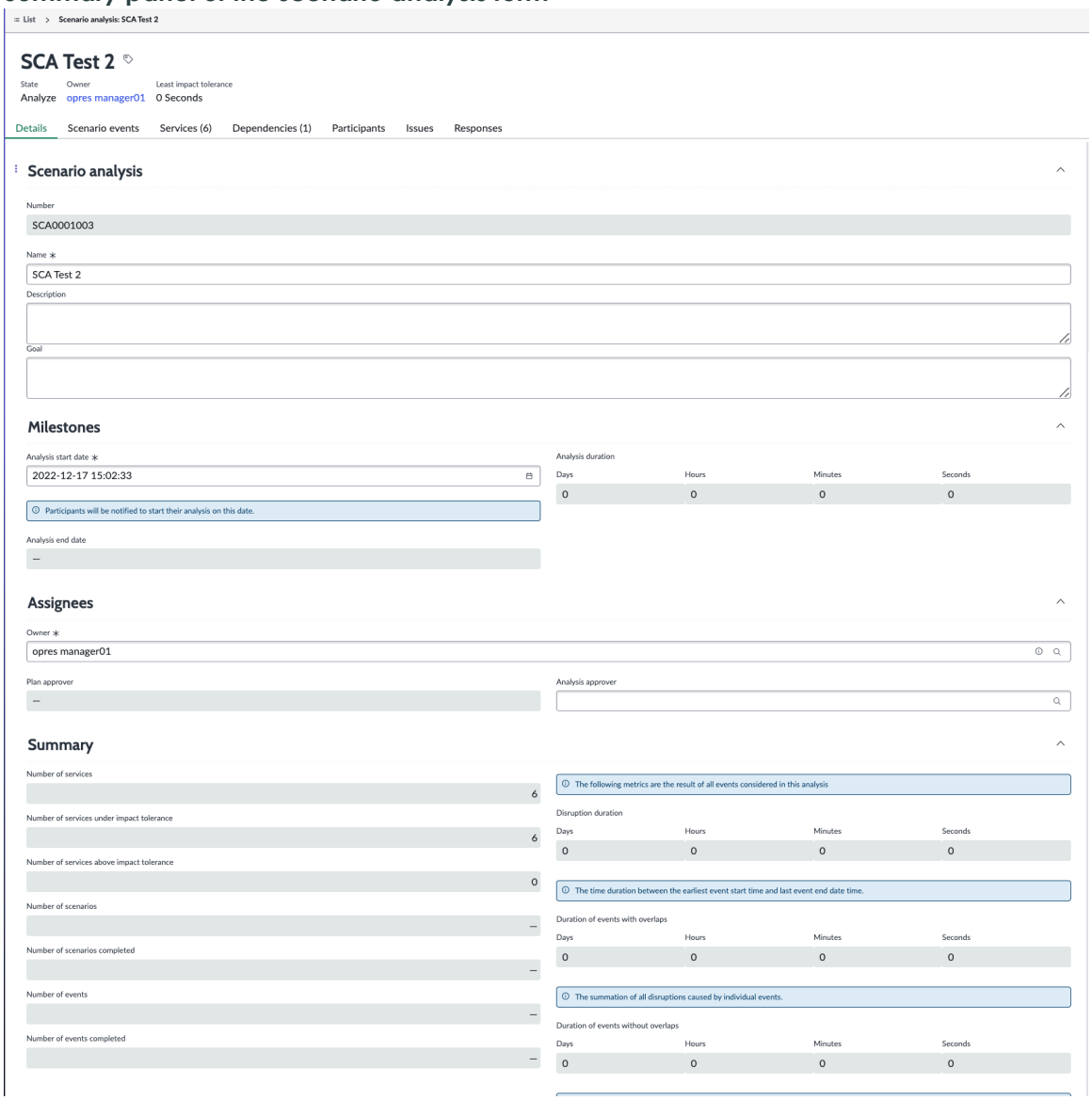
**Note:** You can also choose to proceed with the scenario analysis without a response task.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Summary of the services, scenarios, disruptions, and events

You can view information on the services, scenarios, disruptions, and events in the Summary panel as shown in the following example.

### Summary panel of the scenario analysis form




The Summary panel provides information about the business services, associated scenarios, disruptions, and events. For a description of the field values, see the following table.

### Summary of the services, scenarios, disruptions, and events

| Field | Description |
|---|---|
| Number of services | Number of services that are associated with the scenario analysis. |
| Number of services under impact tolerance | Number of services that are associated with the scenario analysis and that are under the impact tolerance. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Summary of the services, scenarios, disruptions, and events (continued)**

| Field | Description |
|---|---|
| Number of services above impact tolerance | Number of services that are associated with the scenario analysis and that are above the impact tolerance. |
| Number of scenarios | Number of scenarios that are associated with the analysis. |
| Number of scenarios completed | Number of completed scenarios that are associated with the analysis. |
| Number of events | Number of events that are associated with the analysis. |
| Number of events completed | Number of completed events that are associated with the analysis. |
| Disruption duration | Time duration between the end time of the last event and the start time of the first event. It is displayed in the number of days. |
| Duration of events with overlaps | Summary of all event durations including the overlapping events and pauses. It is displayed in the number of days and minutes. |
| Duration of events without overlaps | Summary of all event durations without the overlapping events and pauses. It is displayed in the number of days and minutes. |

### Create a scenario analysis for a business service

Create a scenario analysis for your business services in Operational Resilience Workspace. You can analyze the impact of the scenarios and associated events. You can then calculate the disruptions and determine if any of your services are breached.

## Before you begin

Role required: sn_oper_res.manager

## About this task

If you have the sn_oper_res.manager role, you can create a scenario analysis. Only the owner of the scenario analysis and the user with the sn_oper_res.admin role can edit the analysis. After you review the analysis, you can request an approval. When the analysis is in the **Approved** state, you can close it.

## Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **Lists** > **All scenario analysis** and select **New**.
   The Create New Scenario analysis form is displayed.
2. In the Scenario analysis panel, enter the name, description, and goal for the scenario analysis.
   The number for the scenario analysis is auto-filled by the system.
3. In the **Analysis start date** field in the Milestones panel, enter the start date for the analysis in the *YYYY-MM-DD HH:mm:ss* format.
   A notification is sent to the participants to start their analysis on the Analysis start date.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

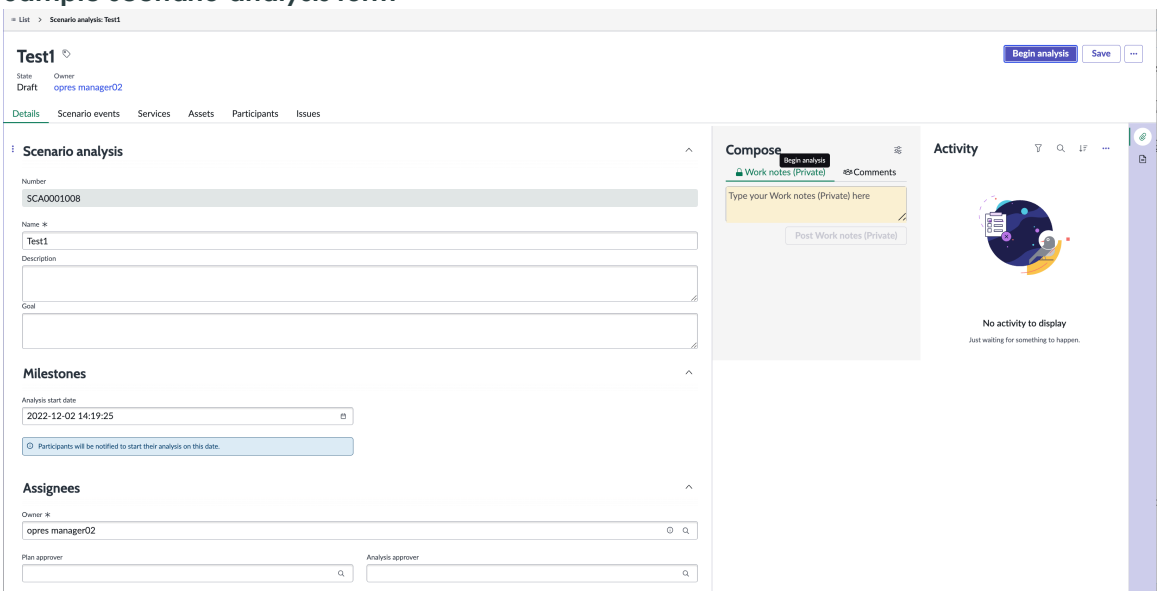
4. In the **Plan approver** field in the Assignees panel, select the plan approver for the analysis.
5. In the **Analysis approver** field, select the analysis approver for the analysis.

   The logged-in user is automatically assigned as the owner of the analysis.

   For the descriptions of the field values on the User New record form, see Create New Scenario analysis form.

   A sample scenario analysis form is shown in the following example.

**Sample scenario analysis form**



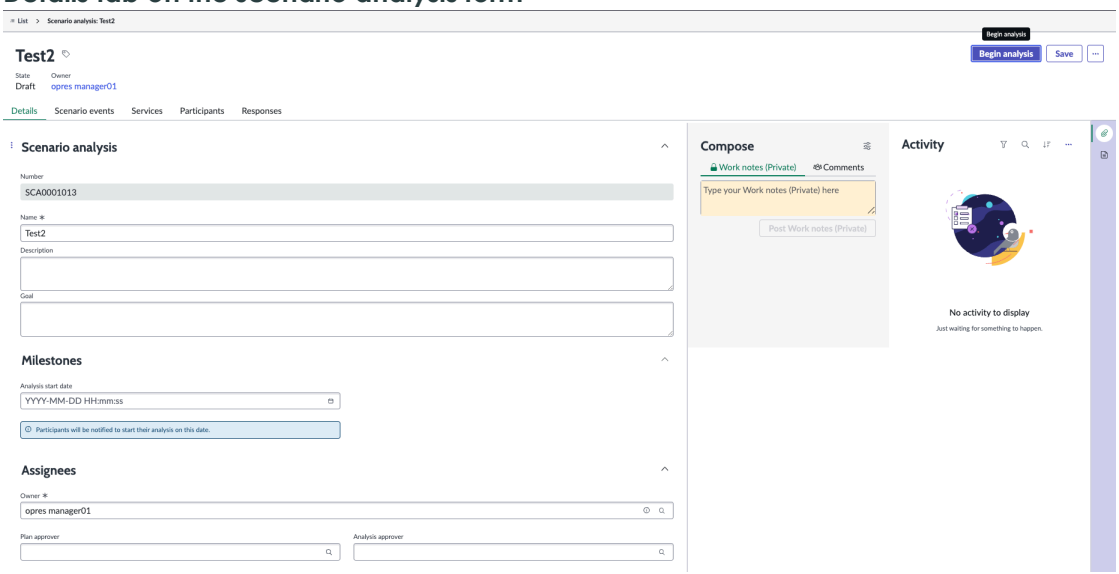

6. Select **Save**.

## Result

You've updated the state of the scenario analysis to **Draft**. The name of the owner is displayed on the form.

The following example shows that on the **Details** tab, you can see the details about the scenario analysis, its important dates, and assignees.

**Details tab on the scenario analysis form**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create New Scenario analysis form

Use the Create New Scenario analysis form in Operational Resilience Workspace to add the details about the scenario analysis, milestones, assignees, and so on.

## Create New Scenario analysis form

For a description of the field values, see the following table.

**Create New Scenario analysis form**

| Field | Description |
|---|---|
| Scenario analysis panel | |
| Number | Number of the scenario analysis. When you create a scenario analysis, the application creates a scenario analysis and assigns it with a unique identification number. This field is auto-filled. |
| Name | Name of the scenario analysis. |
| Description | Description for the scenario analysis. |
| Goal | Specific goal that you want to achieve by performing the scenario analysis. For example, your goal might be to analyze the critical services for your business. |
| Milestones panel | |
| Analysis start date | Date to start the scenario analysis. The owner of the analysis fills in the Analysis start date. A notification is sent to the participants to start their analysis on this date. |
| Assignees panel | |
| Owner | Owner of the scenario analysis. |
| Plan approver | Approver of the scenario analysis plan. |
| Analysis approver | Approver of the scenario analysis. |
| Compose panel | |
| Work notes | Work notes for the activities that are related to the record. |
| Additional comments (Customer visible) | More comments that can be shared with the customer. |
| Activity panel | |
| Activity section | List of activities with the dates and times that are related to the scenario analysis. |
| Tabs associated with the scenario analysis | |
| Scenario Events | **Note:** You must add at least one service, one scenario event, and one participant before proceeding with the scenario analysis.<br><br>Scenario events that an analysis owner can associate with the analysis. As an owner, select **Add** to associate a scenario event with the analysis. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Scenario analysis form (continued)**

| Field | Description |
|---|---|
| | When you add a scenario event to the analysis, the following details about the event are displayed on the form:<br>• Name. For example, Facility outage.<br>• Event group. For example, Infrastructure Events.<br>• Scenario. For example, Flooding Situation.<br>• Pillars. For example, Facilities, People, Suppliers, or Technology.<br>• Potential start date time. For example, the date and time when a user starts working on the event.<br>• Potential end date time. For example, the date and time when a user finishes working on the event.<br>• Duration. For example, the calculated duration of the event.<br>• Observations. For example, the observations about the scenario event.<br>• Gaps. For example, the gaps or missing information about the scenario event.<br>• Recommendations. For example, the recommendations about the scenario event.<br>• Status of the scenario event. |
| Services | Services that an analysis owner can associate with the analysis. As an owner, select **Add** to associate a service with the analysis.<br>When you associate a service with the analysis, the following details about the service are displayed on the form:<br>• Name<br>• Owned by<br>• Importance<br>• Impact tolerance<br>• Disruption duration<br>• Breach status<br>• Deviation (%) |
| Participants | Participants that an analysis owner can add to the analysis. To add a new participant, you can select **New** on the form.<br>When you add a participant to the analysis, the following details about the participant are displayed on the form:<br>• Name<br>• Role<br>• Instruction |
| Dependencies | Assets that are added to a scenario analysis. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Scenario analysis form (continued)**

| Field | Description |
|---|---|
| | When you add an asset to the analysis, the following details about the asset are displayed on the form:<br>• Name of the asset<br>• Associated analysis scenario event |
| Responses | Response task that is associated with the scenario event. The following details are displayed on the Responses form:<br>• Number<br>• Participant<br>• State<br>• Short description<br>• Observation<br>• Gap<br>• Recommendation |
| Issues | Issues that are associated with the scenario analysis. The following details are displayed on the Issues form:<br>• Issue<br>• Number<br>• State<br>• Priority<br>• Assigned to<br>• Issue manager<br>• Scenario event |
| Summary | |
| Number of services | Number of services that are associated with the scenario analysis. |
| Actual start date | Actual start date of the scenario analysis. |
| Actual end date | Actual end date of the scenario analysis. This field is auto-filled. |
| Actual duration | Actual duration of the scenario analysis. This field is auto-filled. |
| Number of services under impact tolerance | Number of services that are associated with the scenario analysis that are under the impact tolerance. |
| Number of services above impact tolerance | Number of services that are associated with the scenario analysis that are above the impact tolerance. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create New Scenario analysis form (continued)

| Field | Description |
|---|---|
| Number of scenarios | Number of scenarios that are associated with the analysis. |
| Number of scenarios completed | Number of completed scenarios that are associated with the analysis. |
| Number of events | Number of events that are associated with the analysis. |
| Number of events completed | Number of completed events that are associated with the analysis. |
| Disruption duration | Time duration between the end time of the last event and the start time of the first event. |
| Duration of events with overlaps | Summation of all event durations including the overlapping events and pauses. |
| Duration of events without overlaps | Summation of all event durations without the overlapping events and pauses. |
| Approvers | Approvers that are associated with the scenario analysis. |

## Add a service to your scenario analysis

Add a service to your scenario analysis so that you can begin to analyze the impact of the scenarios and events in Operational Resilience Workspace.

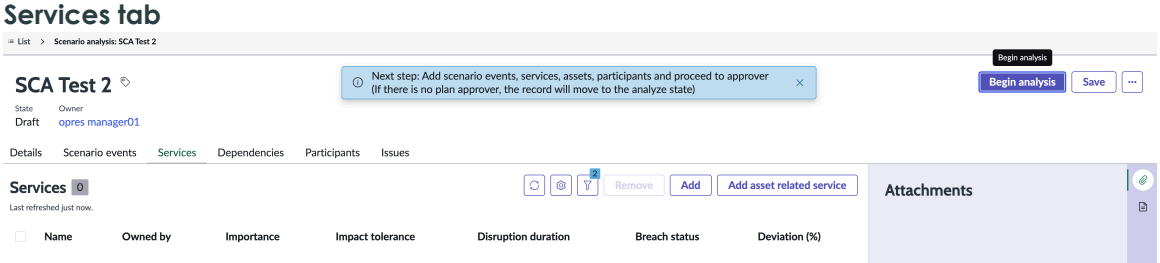
### Before you begin

Role required: sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **All scenario analysis** and then to the scenario that you're working on.
2. On the **Services** tab, select **Add**.
   The **Services** tab is shown in the following example.

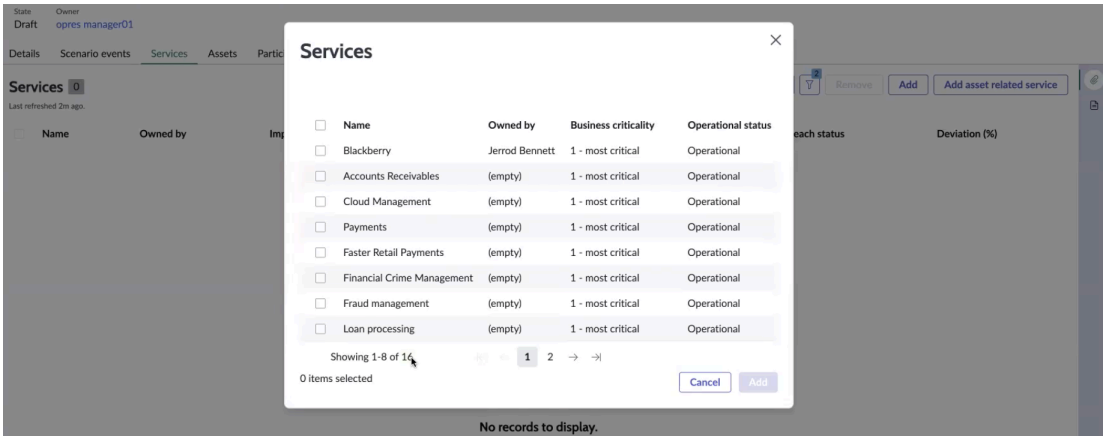
**Services tab**




When you select **Add** in the **Services** tab, it displays a list of all the available services that are fetched from the Services (OR) entity type. A sample list view of the services is shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

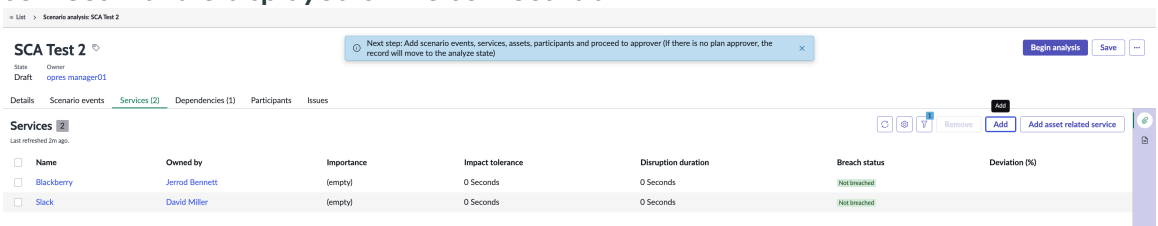
**List view of the services**




**a.** Select one or more services in the list view and select **Add**.

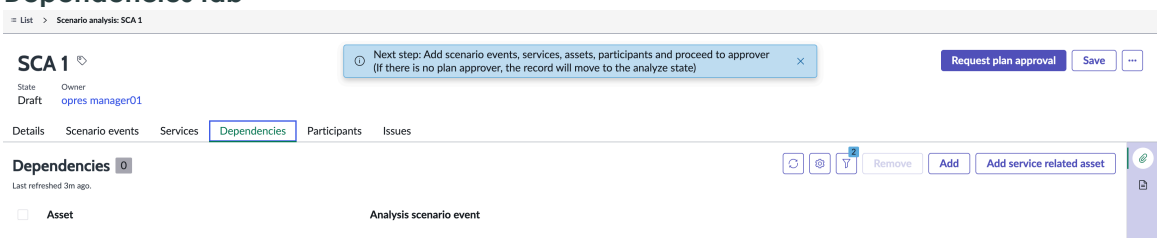
The selected services are displayed on the **Services** tab as shown in the following example.

**Services that are displayed on the Services tab**




**3.** To add a dependency to your scenario analysis, navigate to the **Dependencies** tab and select **Add**.
The **Dependencies** tab is displayed as shown in the following example.

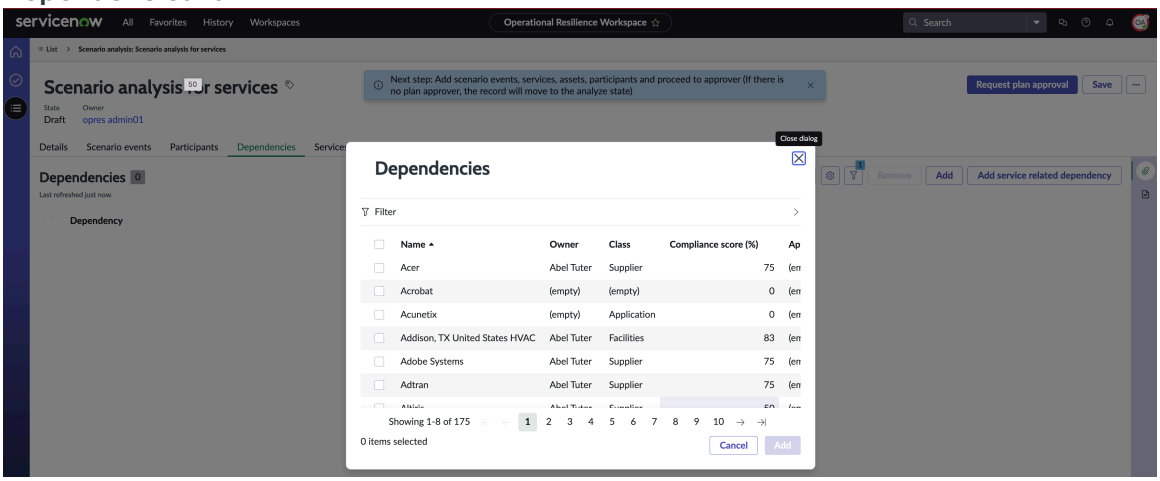
**Dependencies tab**




The Dependencies list on the **Dependencies** tab is displayed as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Dependencies list**



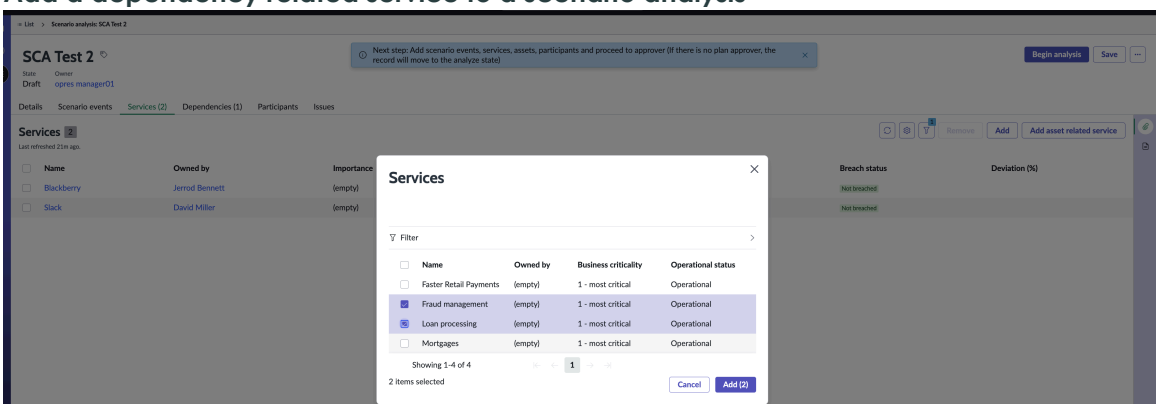

**a.** Select one or more dependencies from the list and select **Add**.
The dependencies are displayed on the **Dependencies** tab.

**4.** To add a service that is related to a dependency, navigate to the **Services** tab and select **Add dependency related service**.

> **Note:** In the Operational Resilience application, some of the services use specific dependencies. You can add the services that are related to a dependency. You must add one or more dependencies on the **Dependencies** tab, as explained in the previous step, before you can add one or more dependency related services to the analysis.

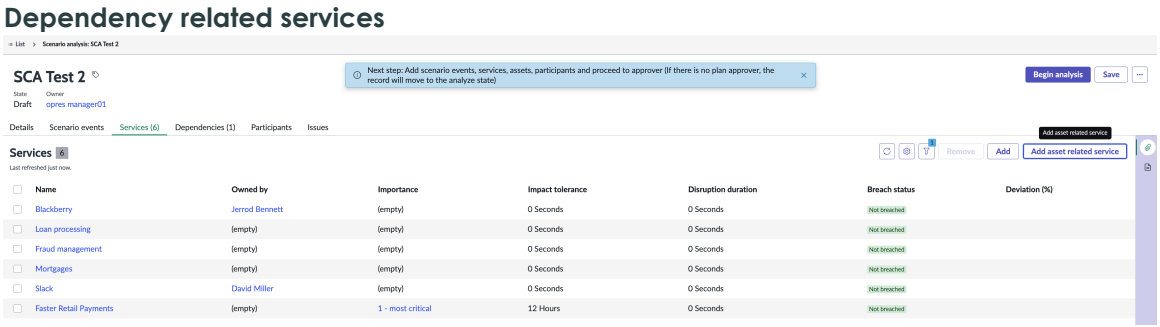
**a.** Select one or more services and select **Add**.
A dependency related services list is displayed as shown in the following example.

**Add a dependency related service to a scenario analysis**




The dependency related services are displayed on the **Services** tab as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




5. Select **Save**.

## Request a plan approval for your scenario analysis

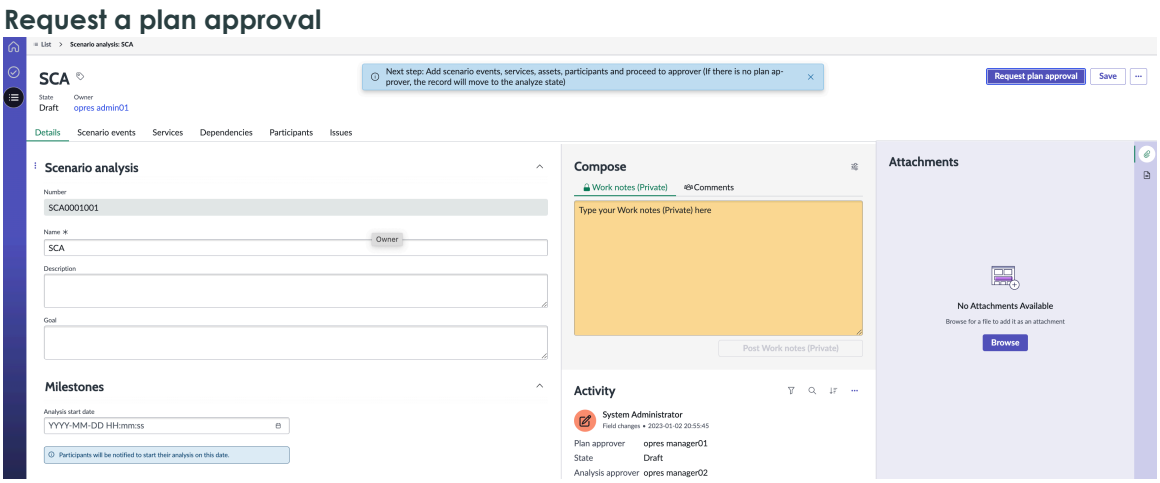
Request a plan approval from the plan approver for your scenario analysis. You can then proceed with the scenario analysis in Operational Resilience Workspace.

### Before you begin

Role required: sn_oper_res.manager

### Procedure

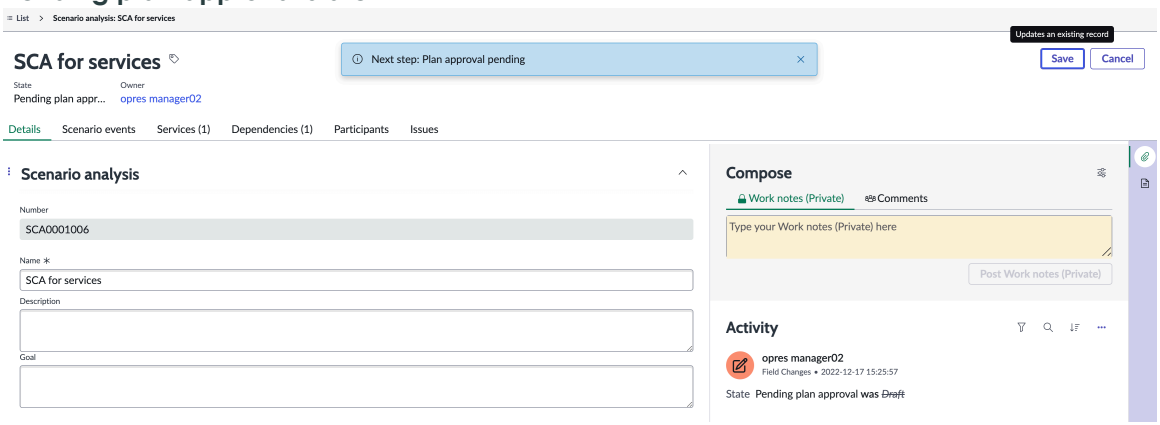
1. Navigate to **All** > **Operational Resilience Workspace** > **All scenario analysis** and select the scenario analysis that you're working on.
2. Select **Request plan approval**.
   You can request a plan approval for the scenario analysis as shown in the following example.




You've updated the state of the scenario analysis to **Pending plan approval**. The state and the owner of the scenario analysis are displayed in the header of the scenario analysis form as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Pending plan approval state




3. Select **Save**.

## Approve the plan for the scenario analysis

Approve the plan for the scenario analysis in Operational Resilience Workspace if you're the plan approver. You can track the actions for the scenario analysis by checking your email notifications.

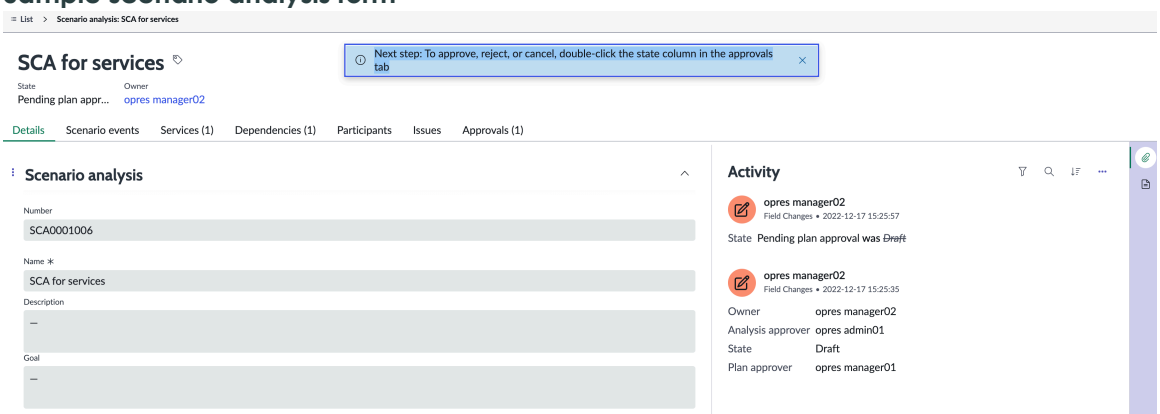
### Before you begin

Role required: sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **All scenario analysis** and select the scenario analysis that you're working on.
2. Log in as the plan approver of the scenario analysis and navigate to the **Approvals** tab. A sample scenario analysis form is shown in the following example.

### Sample scenario analysis form

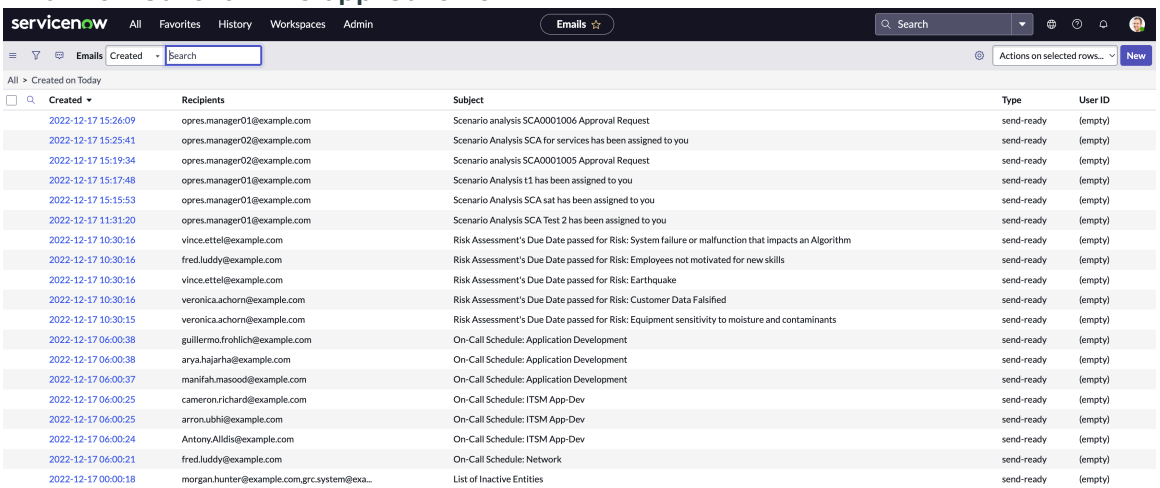



3. Check your emails for notifications.

   a. Log in as an administrator and navigate to **All > Emails** in the application UI. During the execution of a scenario analysis, the email notifications are automatically sent to the owner, approver, and participants. You can view the email notifications as displayed in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

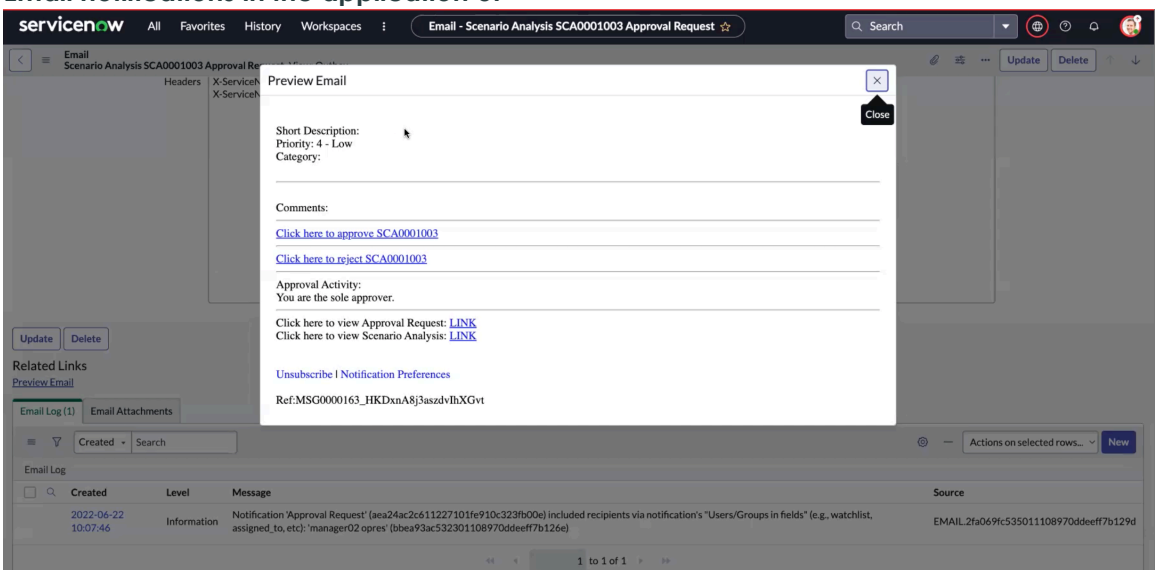
**Email notifications in the application UI**




**b.** Select the email record from the list.

**c.** In the email record, select **Preview Email**.
The Preview Email is displayed as shown in the following example.

**Email notifications in the application UI**



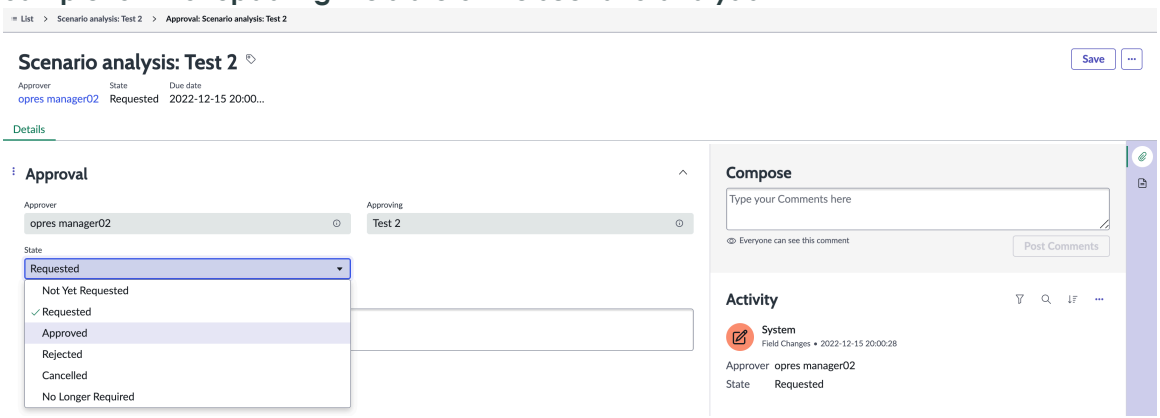

**d.** In the email, select **Approve**.

You can approve or reject the scenario analysis from the **Comments** section or you can view the **Approval Request** links as shown in the example. The approved analysis is updated to the **Analyze** state. The rejected scenario analysis is reset to the **Draft** state.

**4.** To approve, reject, or cancel the scenario analysis, double-click the state column on the **Approval** tab.
A sample form for updating the state of the scenario analysis is shown in the following example.

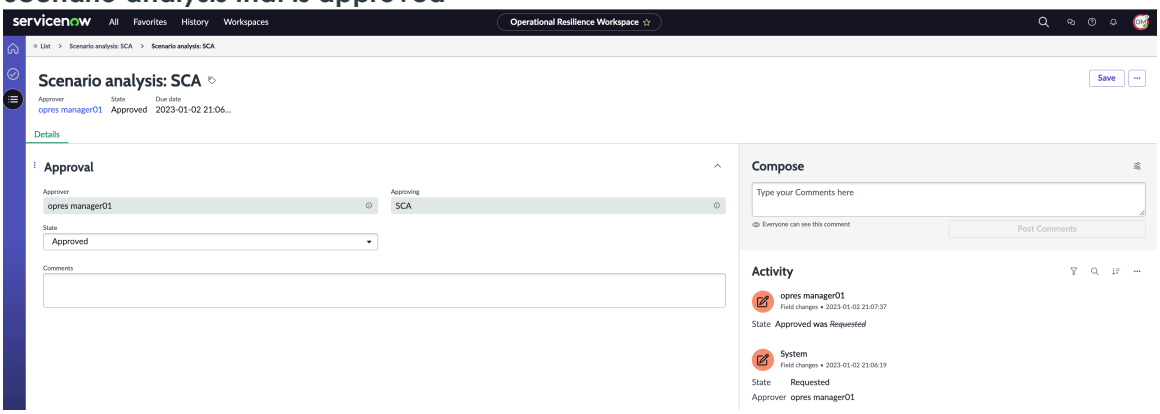
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Sample form for updating the state of the scenario analysis




5. Update the state from **Requested** to **Approved**.
6. In the scenario analysis form, select **Save**.
   As a plan approver, you've approved the scenario analysis as shown in the following example.

### Scenario analysis that is approved




## Add a scenario event and a participant to the scenario analysis

Add a scenario event and a participant to your scenario analysis so that you can analyze the impact of the scenario event on your business service. By collating the observations from the participants in Operational Resilience Workspace, you can determine the impact of the scenario event on a business service.

### Before you begin

Role required: sn_oper_res.manager

### Procedure

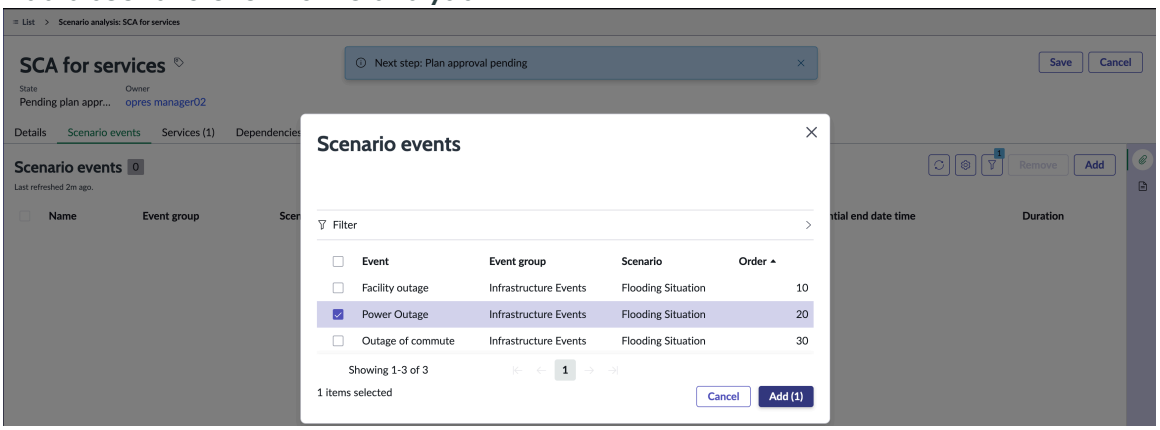
1. Navigate to **All** > **Operational Resilience Workspace** > **All scenario analysis** and select the scenario analysis that you own.
2. On the **Scenario events** tab, perform the following tasks.

   a. Select **Add**.

   b. In the Scenario events form, select an event from the list and select **Add**.
   The sample scenario events list is shown in the following example.

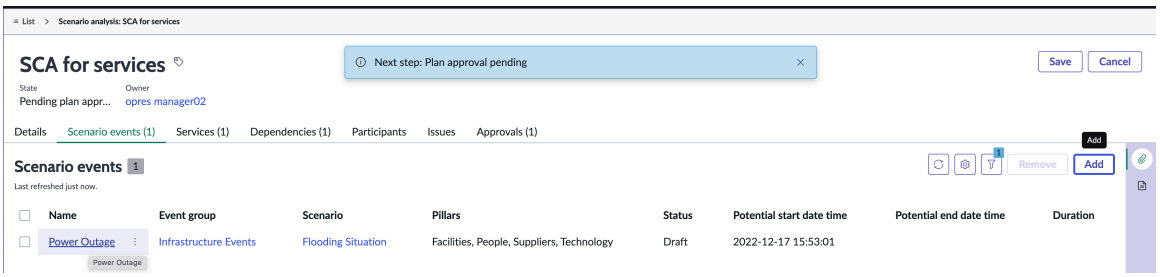
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Add a scenario event to the analysis




In the **Scenario events** tab, the selected scenario event is displayed as shown in the following example.

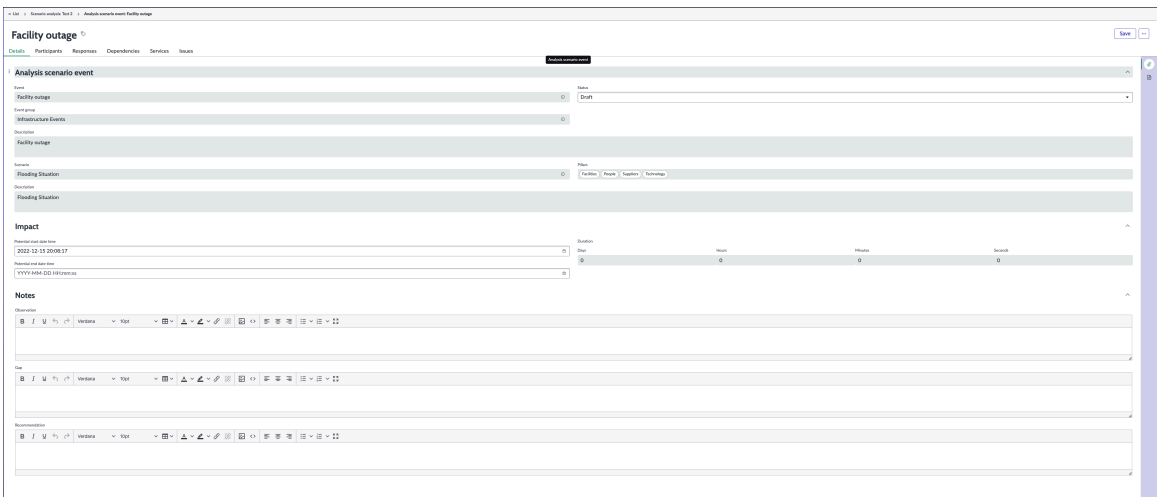
### Scenario event in the list




For the descriptions of the field values on the Scenario event form, see Scenario event form.

3. Open the scenario event from the list.
   The scenario event form is displayed as shown in the following example.

### Scenario event form




4. On the **Dependencies** tab, add a dependency for the scenario event.
5. On the **Services** tab, add a service for the scenario event.
6. On the **Issues** tab, select the issues that are associated with the event.

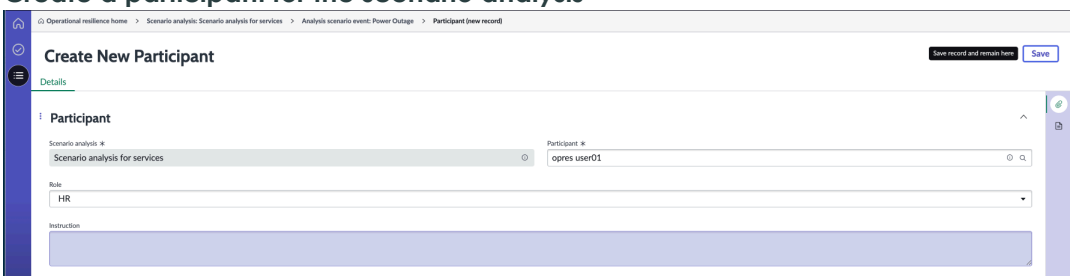
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Navigate to the **Participants** tab in the scenario event form and then either add a participant from an available list or add a new participant.

| Step | Description |
|---|---|
| Select **Add**. | Add a participant from the available list of participants for the scenario analysis. |
| Select **New**. | Add a new participant to the scenario event. |

a. Select **New**.
The Create New Participant form is displayed as shown in the following example.

**Create a participant for the scenario analysis**




The name of the scenario analysis is auto-filled by default.

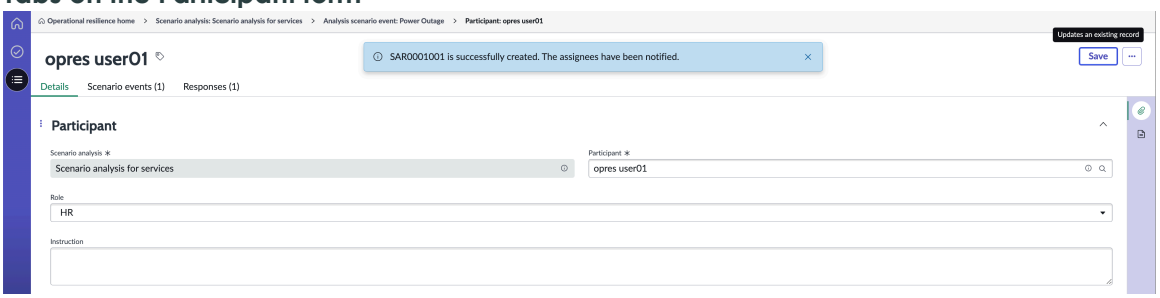
b. In the **Participant** field, select a participant from the list in the Participant form.
When you select a participant, the role is auto-filled in the Role field.

c. In the **Instruction** field, add instructions for the participant.

d. Select **Save**.

You can view the tabs on the Participant form as shown in the following example.

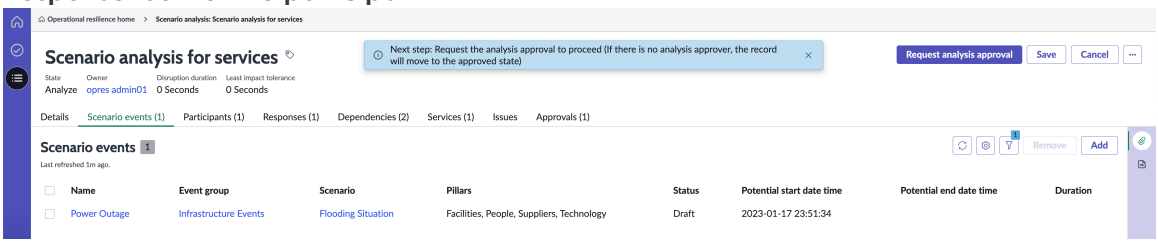
**Tabs on the Participant form**




When you create a scenario event and add a participant to it, a response task is automatically created for the participant. The following example shows that when a participant is assigned to added to a scenario event, a response task is created.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

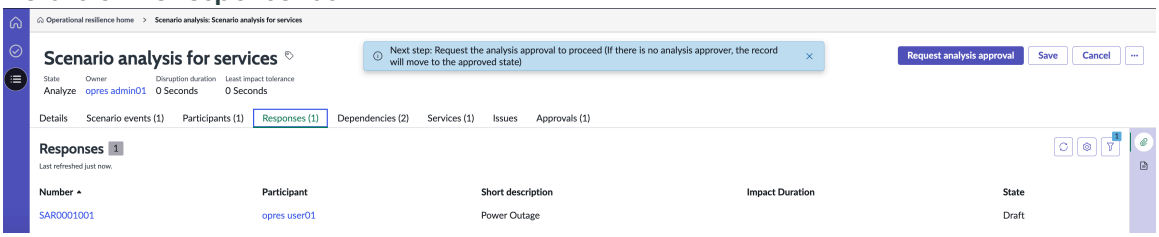
**Response task for the participant**




An email notification is automatically sent to the participant.

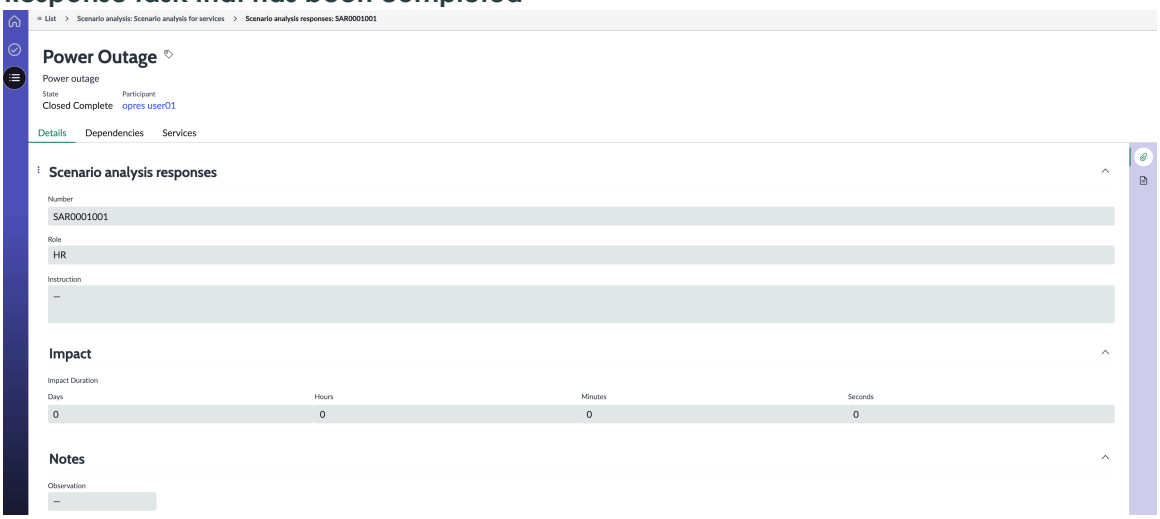
On the **Responses** tab, the details of the response task such as the response task number, name of the assigned participant, and state of the response task are displayed as shown in the following example.

**Details of the response task**



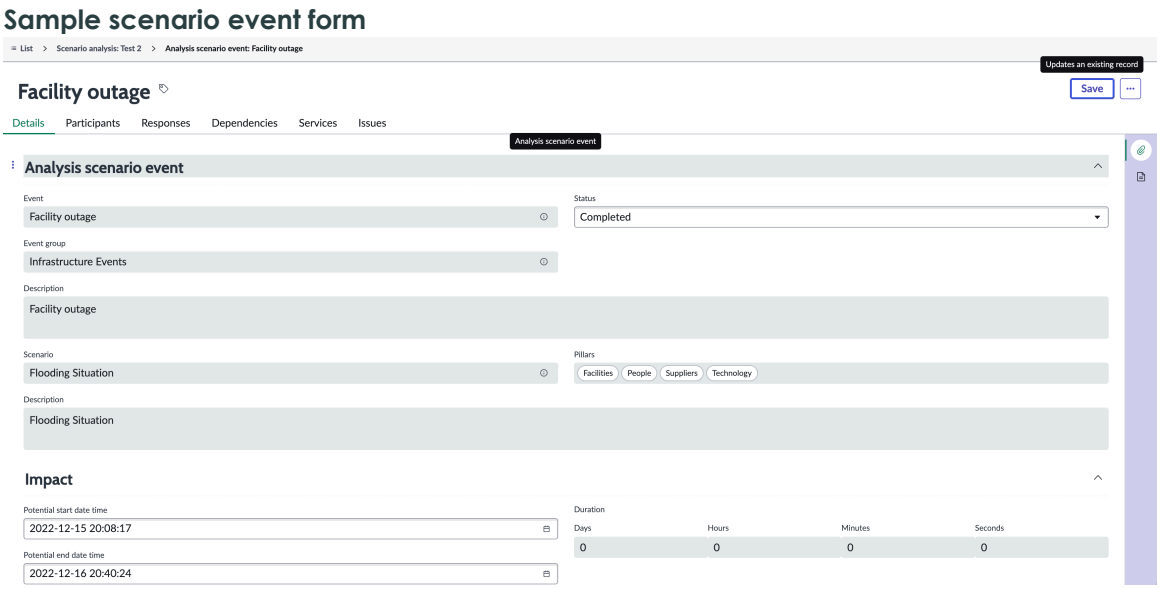

8. On the **Responses** tab, select the response task and on the form, fill in the fields.
   For the descriptions of the field values on the Scenario event form, see Scenario event form.
9. Complete the open response task and select **Complete**.
   The response task is completed and the state of the response task is updated to **Closed Complete** as shown in the following example.

**Response task that has been completed**

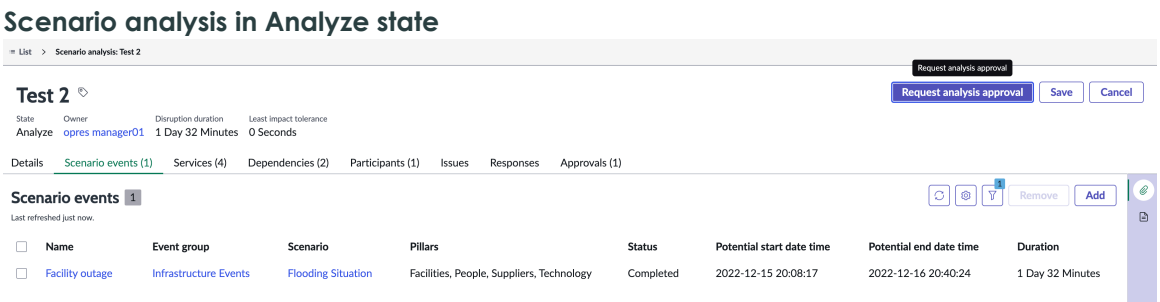



10. Log in as an owner of the scenario analysis, navigate to the open scenario event, and update its state from **Draft** to **Completed**.
11. Update the **Potential start date time** and **Potential start date time**.
    A sample scenario event form is shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

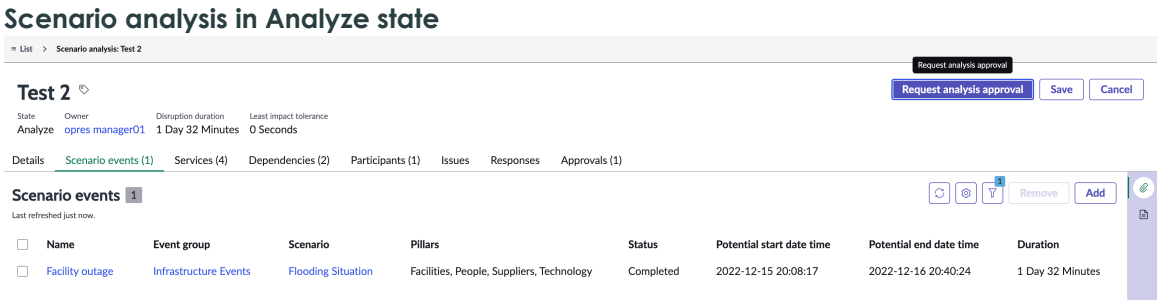



You've updated the state of the scenario analysis to **Analyze** as shown in the following example.




## Result

You've updated the state of the scenario analysis to **Analyze** as shown in the following example.




### Scenario event form

Use the Scenario event form in Operational Resilience Workspace to associate a scenario event with your scenario analysis.

## Scenario event form

For a description of the field values, see the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Scenario event form

| Field | Description |
|---|---|
| Details tab | |
| Analysis scenario event panel | |
| Event Name | Unique name for the event. This field is auto-filled. |
| Event group | Unique name for the event group. This field is auto-filled. |
| Status | Status of the event. Available options are:<br>• Draft<br>• Completed |
| Description | Description of the event. This field is auto-filled. |
| Scenario | Scenario associated with the event. This field is auto-filled. |
| Pillars | Pillars associated with the event. This field is auto-filled. |
| Description | Description of the event. This field is auto-filled. |
| Impact panel | |
| Potential start date time | Potential start date and time for the event. This field is auto-filled. |
| Potential end date time | Potential end date and time for the event. |
| Duration | Duration of the event. This field is auto-filled. |
| Notes | |
| Observations | Observations added for the event by the participant. |
| Gaps | Gaps added for the event by the participant. |
| Recommendations | Recommendations added for the event by the participant. |
| Participants tab | |
| Scenario analysis | Scenario analysis that is associated with the scenario event. This field is auto-filled. |
| Role | Role of the participant. Available options are:<br>• HR<br>• Legal<br>• Finance<br>• Technology |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Scenario event form (continued)**

| Field | Description |
|---|---|
| | • People<br>• Data<br>• Security<br>• Supplier Tier1<br>• Supplier Tier2<br>• Supplier Tier3 |
| Participant | Participant of the scenario analysis such as Operational Resilience administrator or manager. |
| Instruction | Text box for adding the instructions for the participants of the scenario event. |
| Responses | Details about the response task such as its number, participant, impact duration, state, and so on. |
| Dependencies | Dependencies (assets) that are associated with the scenario event. |
| Services | Services that are associated with the scenario event. |
| Issues | Issues that are associated with the scenario event. |

### Scenario analysis response task form

Use the Scenario analysis response task form in Operational Resilience Workspace to add the details about the response task that is associated with a scenario event.

## Scenario analysis response task form

For a description of the field values, see the following table.

**Scenario analysis response task form**

| Field | Description |
|---|---|
| Scenario Analysis Response panel | |
| Number | Number of the scenario analysis response task such as SAR0001006. This field is auto-filled. |
| Role | Role of the assignee of the response task. |
| Instruction | Instruction for the assignee of the response task. |
| Impact panel | |
| Impact duration | Impact duration of the scenario event in Days, Hours, Minutes, and Seconds. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Scenario analysis response task form (continued)

| Field | Description |
|---|---|
| Notes panel | |
| Observations | Observations about the scenario event that are added by the assignee of the response task. |
| Gaps | Gaps or inconsistencies about the scenario event that are added by the assignee of the response task. |
| Recommendations | Recommendations about the scenario event that are added by the assignee of the response task. |
| Scenario analysis panel | |
| Scenario analysis | Name of the scenario analysis. |
| Pillar | Pillars that are associated with the scenario analysis. |
| Description | Description of the scenario analysis. |
| Goal | Goal for performing the scenario analysis. |

## Associate an issue with the scenario analysis

Associate an issue with your scenario analysis by creating an issue or adding an existing issue to the scenario analysis. You can then measure the gaps in your resilience metrics and define a plan of action to mitigate the gaps.

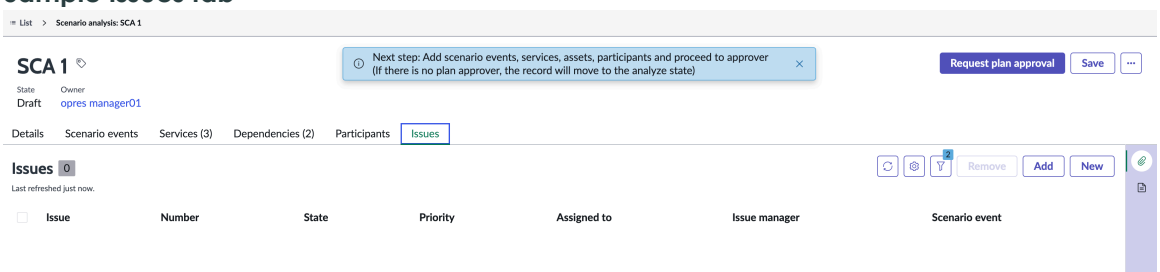
### Before you begin

Role required: sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **All scenario analysis** and select the scenario analysis that you're working on.
2. In the scenario analysis form, navigate to the **Issues** tab.
   A sample **Issues** tab is shown in the following example.

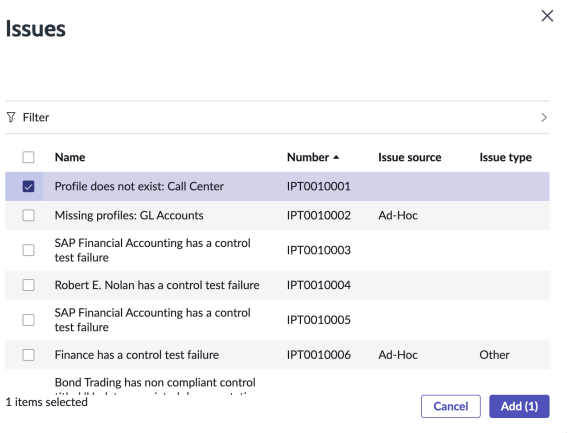
**Sample Issues tab**




You can add an existing issue to the analysis or create an issue that you can add to the analysis.

**Note:** If you've associated an open issue with your scenario analysis, you can still request an approval for the scenario analysis. It isn't required to close the open issues for requesting an approval for the scenario analysis.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Step | Description |
| --- | --- |
| Select **Add**. | Add an existing issue to the analysis. The following example shows how to add an existing issue to the analysis.<br>**Add an existing issue to the analysis**<br>  |
| Select **New**. | Create an issue that you can add to the scenario analysis. The following example shows how to create an issue that you can add to the scenario analysis.<br>**Create an issue that you can add to the scenario analysis**<br>  <br>For the descriptions of the field values on the Create New Issue form, see Create New Issue form. |

3. Select **Save**.

### Request an analysis approval for the scenario analysis

Request an analysis approval for the scenario analysis in Operational Resilience Workspace. With an approval, you can then close the scenario analysis.

**Before you begin**
Role required: sn_oper_res.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

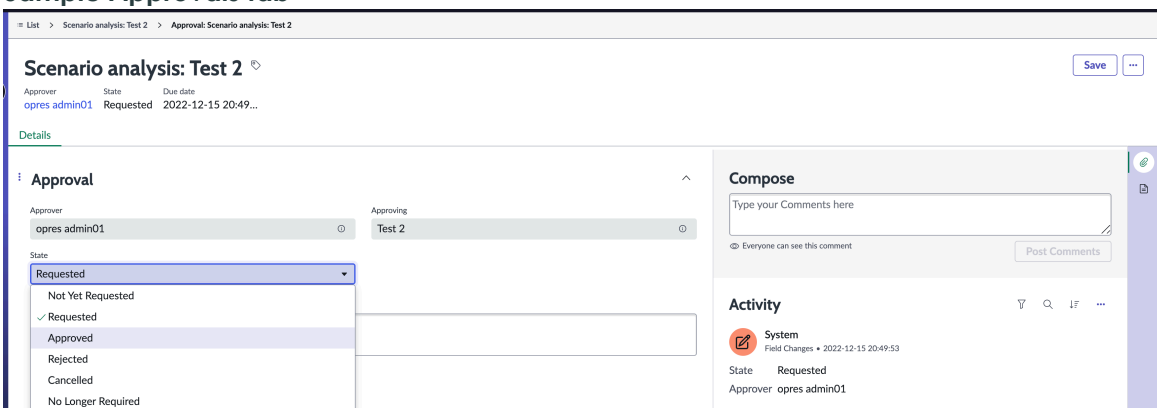
## Procedure

1. Navigate to the scenario analysis that you're working on in one of the following ways:
   - **All** > **Operational Resilience Workspace** > **All scenario analysis**
   - **All** > **Operational Resilience Workspace** > **Tasks** > **Scenario analysis approvals**

   If you navigate to the scenario analysis from the Tasks page, you can skip steps 2 and 3 and update the state of the scenario analysis as outlined in step 4.

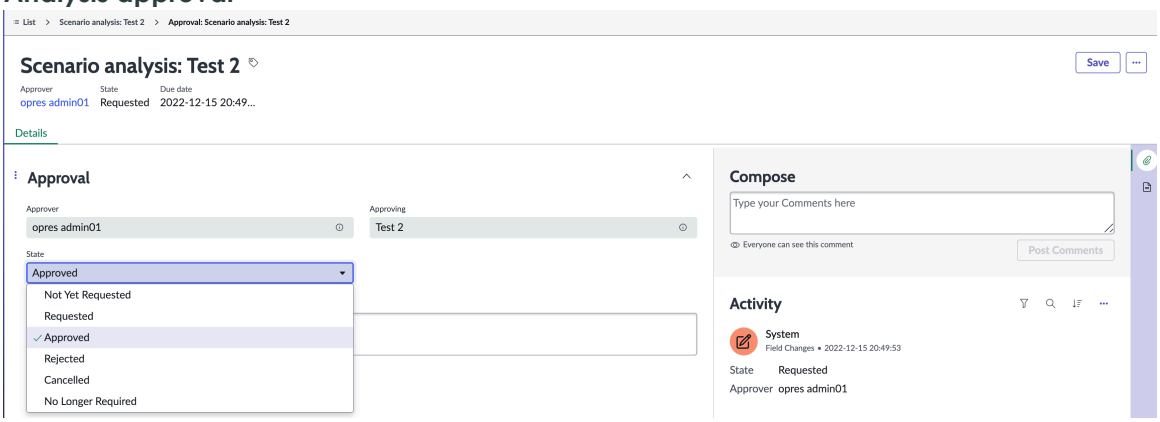
2. Select **Request plan approval**.
   The state of the scenario analysis is updated to **Pending analysis approval**.
3. Log in as the analysis approver for the scenario analysis and navigate to the scenario analysis in the List view.
   A sample **Approvals** tab is shown in the following example.

**Sample Approvals tab**




4. In the **State** field, update the state from **Requested** to **Approved**.
   A sample form for updating the approval is shown in the following example.

**Analysis approval**

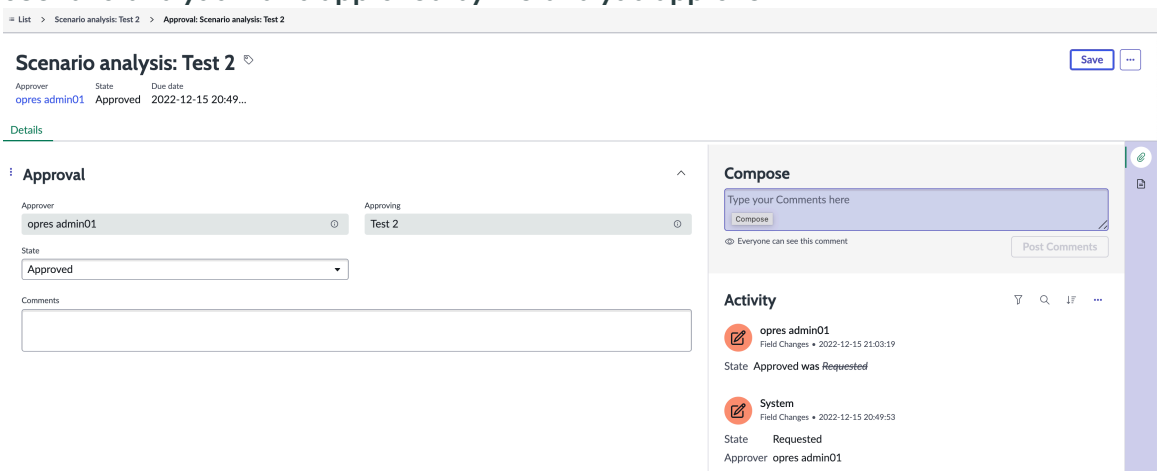



5. Select **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

As an analysis approver, you've approved the scenario analysis as shown in the following example.

**Scenario analysis that is approved by the analysis approver**




## Close the scenario analysis

Close the scenario analysis in Operational Resilience Workspace. After closing the scenario analysis, you can share your observations and notes with the stakeholders.

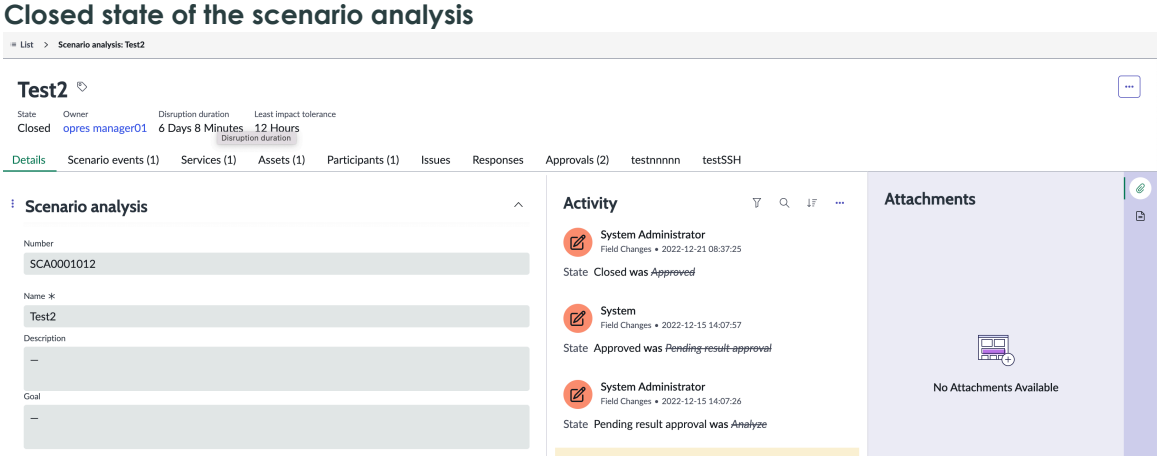
### Before you begin

Role required: sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **All scenario analysis** and select the scenario analysis that has been approved.
2. Select **Close**.
   This action completes the scenario analysis workflow.
   As an owner of the scenario analysis, you've closed the scenario analysis as shown in the following example.

**Closed state of the scenario analysis**




## Self-attesting the business services in Operational Resilience Workspace

If you have the sn_oper_res.manager role, you can certify the operational resilience status of your business services by completing the self-attestation process in Operational Resilience Workspace. You can complete the self-assessment questionnaire about the services,

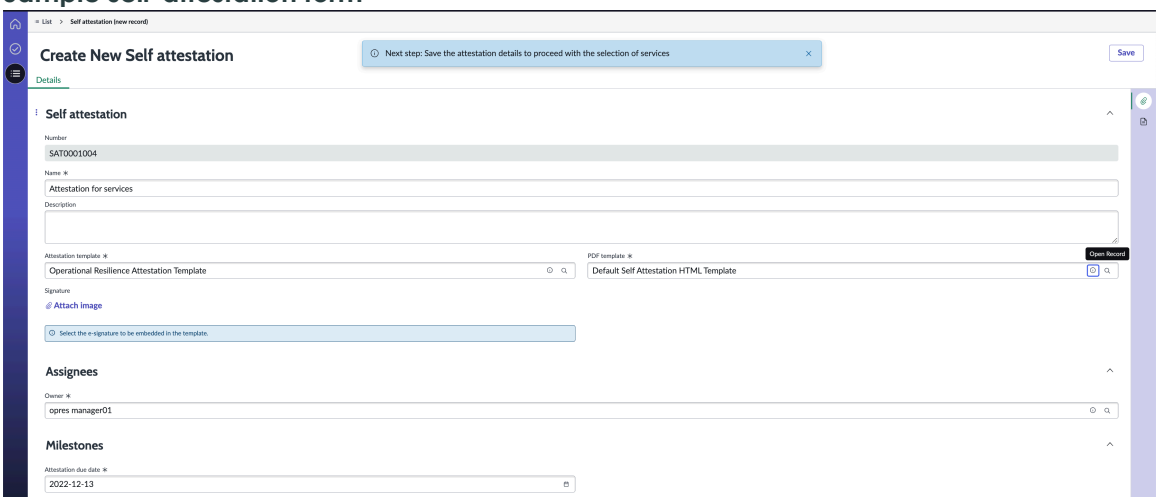
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

generate a self-attestation report, and upload the PDF so that you can have a copy of the report for your records.

## Creating a self-attestation

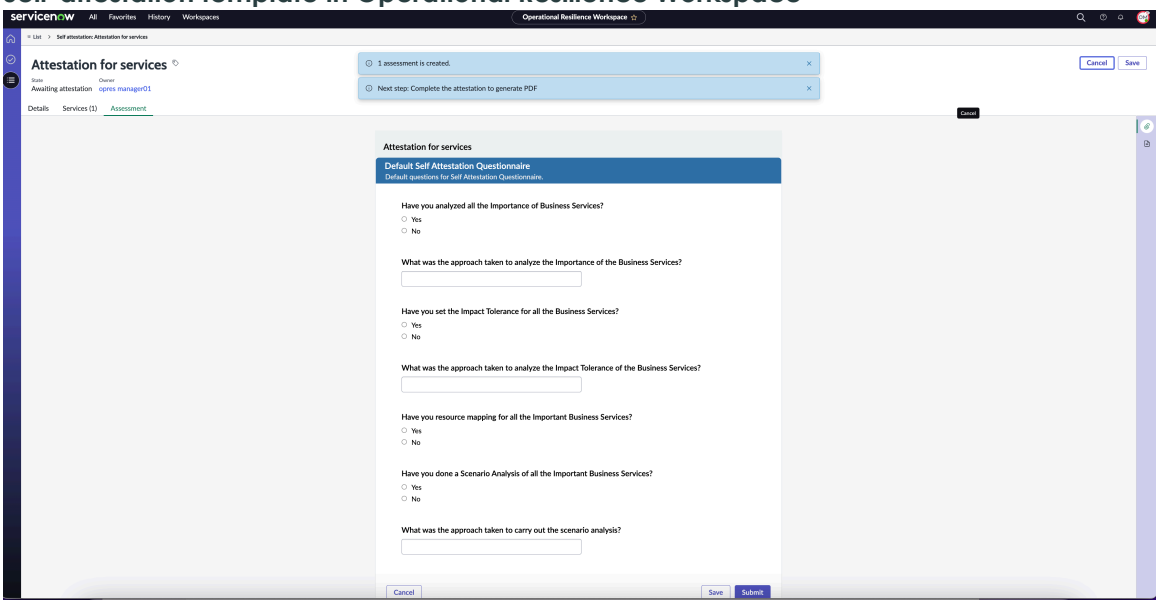
To create a self-attestation in the Operational Resilience application, navigate to **All** > **Operational Resilience Workspace** > **All self attestations** in an instance. A sample self-attestation form is shown in the following example.

### Sample self-attestation form




You can submit an assessment on the services by using the self-attestation template that is provided in Operational Resilience Workspace as shown in the following example.

### Self-attestation template in Operational Resilience Workspace




## Self-attestation tasks and the states related to each task

With the sn_oper_res.manager role, you can complete the following self-attestation tasks in Operational Resilience Workspace:

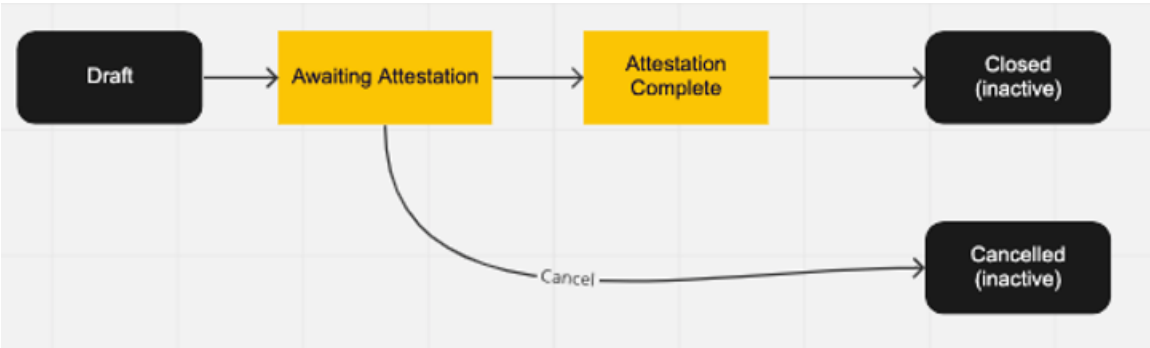
1. Initiate a self-attestation to attest one or more business services.
2. Select the Operational Resilience Attestation Template as the attestation template.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Use the Default Self Attestation HTML Template as the PDF template for the self-attestation in the self-attestation form. This template provides the format for the PDF and an option to include your e-signature in the report.
4. Add the services that you want to certify the status for in the self-attestation form. Respond to the pre-defined set of questions in the assessment, such as the names and description of the services, details on the scenario analysis of the important services, your approach for the scenario analysis, and so on.
5. Submit the assessment and attest for the services.
6. Download a PDF of the self-attestation from the Activity section of the self-attestation form and save a copy of the report for your records.
7. Close the self-attestation so that the self-attestation process is complete.

When you complete the self-attestation tasks that are described in the self-attestation process, the states related to the self-attestation tasks are updated automatically in a sequence as shown in the following example.

**States that are related to the self-attestation tasks**




The states and UI actions that are related to the self-attestation tasks are explained in the following table.

**States and UI actions related to the self-attestation tasks**

| States | Associated UI actions | Description |
|---|---|---|
| Draft | Select **New** in the self-attestation form. | When you select **New** to submit a self-attestation for the services, a record is created in the **Draft** state by default. The information on the self-attestation is displayed on the **Details** tab in the self-attestation form. |
| Awaiting attestation | Select **Attest** in the self-attestation form. | When you select the services that you want to certify, you can choose the attestation template and select **Attest** to proceed with the attestation. The application then creates an assessment instance |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and UI actions related to the self-attestation tasks (continued)**

| States | Associated UI actions | Description |
|---|---|---|
| | | automatically on the **Assessment Instances** tab.<br><br>This action moves the state of the self-attestation record to **Awaiting attestation**.<br><br>**Note:** To proceed with the attestation process, you must associate at least one service with the self-attestation. |
| Cancelled | In the self-attestation form, select **Cancel** . | When the self-attestation record is in the **Awaiting Attestation** state, you can cancel an erroneous or invalid attestation by selecting **Cancel** in the self-attestation form. This is an optional step. The state of the self-attestation is then updated to **Cancelled**. |
| Attestation received | In the attestation template, select **Submit** and select **Save** to complete the attestation process. Select **Export to PDF** to export the questionnaire response to a PDF. | When the self-attestation record is in the **Awaiting attestation** state, you can respond to the assessment questions that are given in the attestation template. To submit the responses, select **Submit** and then select **Save** to save the assessment. The state of the self-attestation is automatically updated to **Attestation received**.<br><br>Select **Export to PDF** to export the questionnaire response to a PDF, sign the self-attestation, and save a copy for your records. You can download the PDF from the Activity section of the self-attestation form. |
| Closed | Select **Close** in the self-attestation form. | To close the attestation, select **Close** in the self-attestation form. The state |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States and UI actions related to the self-attestation tasks (continued)**

| States | Associated UI actions | Description |
|---|---|---|
| | | of the self-attestation is then updated to **Closed**. |

**Note:** Optionally, if the self-attestation contains invalid data and you're the owner of the self-attestation, you can delete the self-attestation by selecting **Delete** in the self-attestation form. The self-attestation is then deleted from the self-attestations list in Operational Resilience Workspace.

## Downloading the PDF of the self-attestation

As an owner of the self-attestation, you can download the PDF from the Activity section of the self-attestation form. You can also share it offline with the auditors, external contacts, or stakeholders.

## Roles required to perform the self-attestation tasks

If you're a user of Operational Resilience Workspace, you can perform different self-attestation tasks with the following roles:

- With the sn_oper_res.admin role, you can create and maintain the pre-defined assessment questionnaire templates.
- With the sn_oper_res.manager role, you can complete the self-attestation of the operational resilience profile of the services by selecting one or more services, by choosing the template for the self-attestation, and by providing the answers to a pre-defined set of questions.

**Note:**

If you're the owner of the self-attestation with the Operational Resilience manager or the Operational Resilience administrator role, you can create a self-attestation, update its details, or delete the self-attestation.

As an Operational Resilience administrator, you can create and modify the assessment questionnaire template. You must have the Operational Resilience manager role to respond to the assessment questionnaire in the Operational Resilience application.

## Reference information

For more information on submitting a self-attestation in Operational Resilience Workspace, see Create an assessment for a self-attestation.

For the description of the field values that are listed in the self-attestation form in the Operational Resilience Workspace, see Create New Self attestation form.

As an optional task, when you have the sn_oper_res.admin role, you can create a customized attestation template instead of using the default attestation template that is provided with the base system. For more information on creating a customized attestation template, see Create and edit an attestation template.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Create an assessment for a self-attestation

Create an assessment for a self-attestation so that you can certify the resilience status of the services in Operational Resilience Workspace. You can use the attestation template that is provided with the base system to create a self-attestation.

### Before you begin

Role required: sn_oper_res.manager

### Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **All self attestations**.
2. Click **New**.
3. Navigate to the **Details** tab in the Create New Self attestation form.
4. In the **Name** and **Description** fields, enter the name and description for the self-attestation.
5. In the **Owner** field, select the owner of the self-attestation.

   For a description of the field values on the self-attestation form, see Create New Self attestation form.

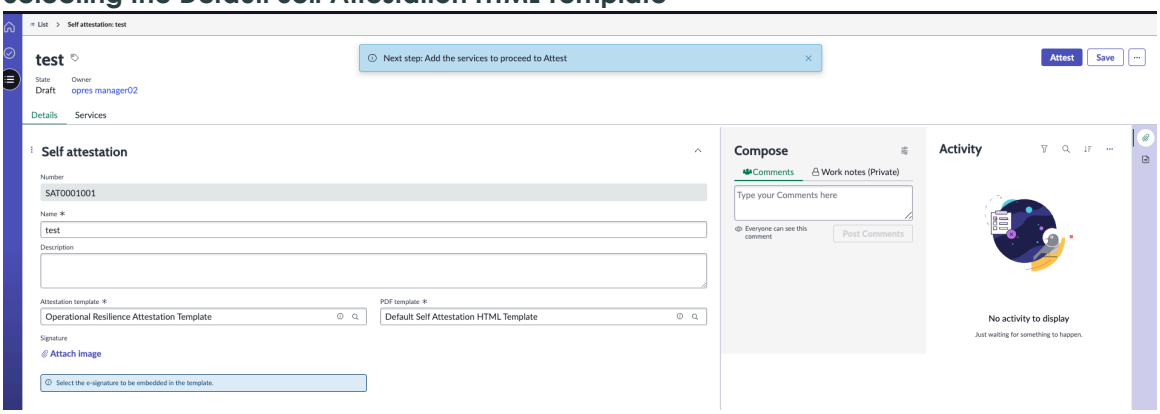
6. In the **Attestation Template** field, select the **Operational Resilience Attestation Template** option.

   The attestation template contains the pre-defined questions for the assessment. The Operational Resilience application provides an attestation template as part of the base system.

   **Note:** If you have the sn_oper_res.admin role, you can customize the default attestation template for your own business needs. For information on creating a customized attestation template, see Create and edit an attestation template.

7. In the **PDF Template** field, select **Default Self Attestation HTML Template**.
   You can use the Default Self Attestation HTML Template so that you can generate a PDF of the self-attestation. The sample self-attestation form is shown in the following example.

   **Selecting the Default Self Attestation HTML Template**




   **Note:** Ensure that you have installed Document Templates on your instance so that the PDF template option is visible in the self-attestation form.

8. In the **Signature** field, click **Attach image** to attach the signature image for the self-attestation.
   The following informational message is displayed: *`Select the e-signature to be embedded in the template.`*

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** You must select the supported file format, such as either the JPEG, PNG, BMP, GIF, ICO, SVG format, for the signature image. If you select a file format that is not supported, such as the Microsoft Word format, the following error message is displayed on the screen: *Selected file type is invalid. Valid field types: JPEG, PNG, BMP, GIF, ICO, SVG.*

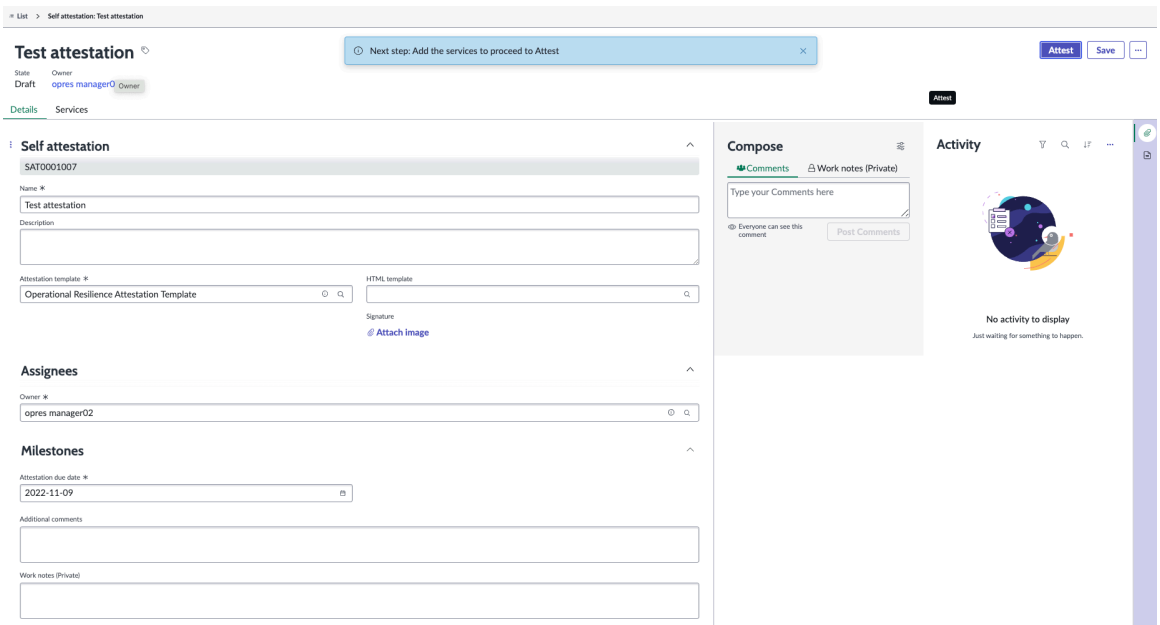
If you want to delete an existing image and add a new image instead, you can use the Delete icon in the **Signature** field and add another signature image as shown in the following example.

### Using the Delete icon to delete the signature image

9. In the Assignees panel, update the **Owner** field to select the owner of the self-attestation.
10. In the Milestones panel, add the attestation due date, additional comments, and work notes (private).
    The following informational message is displayed on the screen: *Next step: Save the attestation details to proceed with the selection of services.*
11. Click **Save**.
    The self-attestation details are saved in the application.

    You have created a self-attestation in the **Draft** state as shown in the following example.

### Self attestation in the Draft state




The **Details** tab is updated with the self attestation information and the **Services** tab is displayed for the self-attestation.

12. Navigate to the **Services** tab.
    You can select one or more services that you want to certify the status for in the self-attestation.

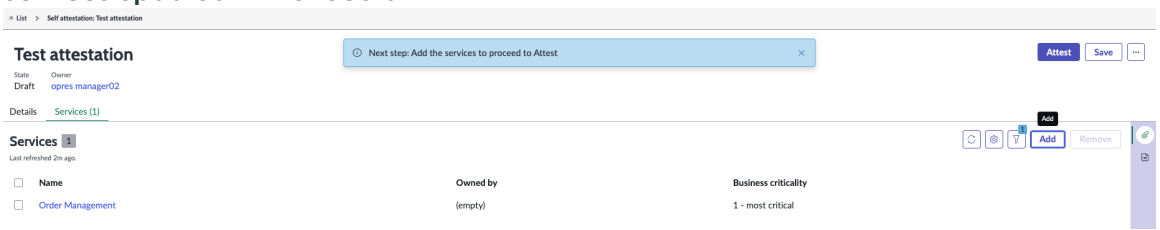
**Note:** You must add at least one service to proceed with the self-attestation.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**a.** Click **Add**.

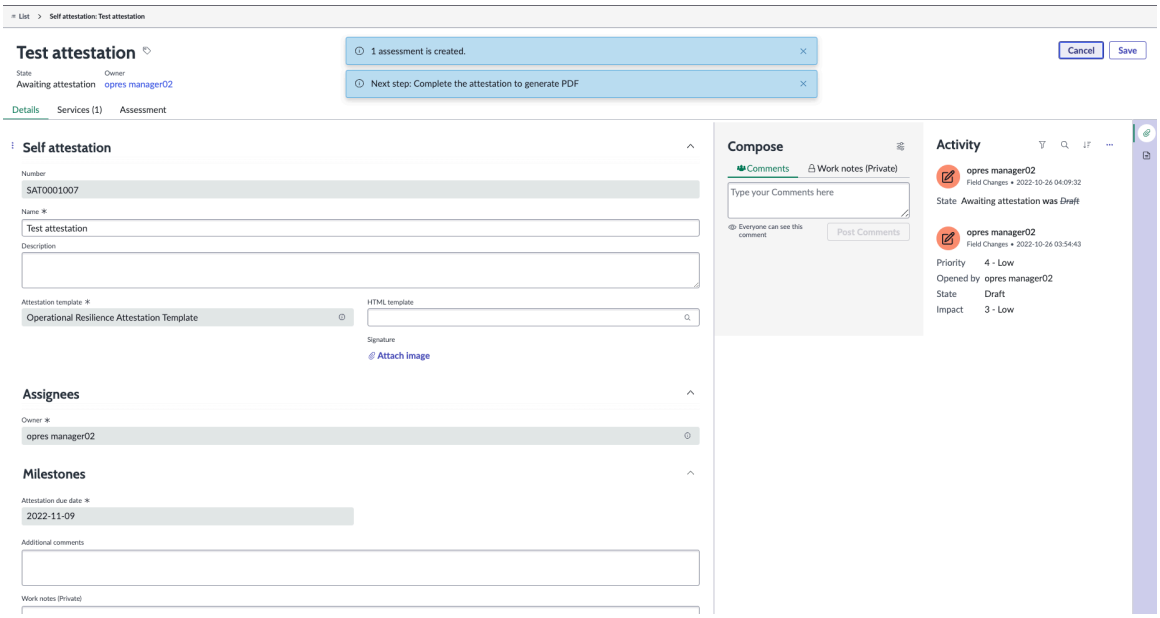
**b.** In the Services form, select a service from the list and click **Add**.
In the Services list, the selected service is displayed as shown in the following example.

**Services updated in the record**




13. Click **Attest**.
You have created an assessment for a self-attestation in the **Awaiting attestation** state as shown in the following example.

**Assessment created for a self-attestation**




### Create New Self attestation form

If you're the owner of the self-attestation, use the Create New Self attestation form in Operational Resilience Workspace to submit the self-attestation for the services.

## Create New Self attestation form

For a description of the field values on the form, see the following table.

**Create New Self attestation form**

| Field | Description |
|---|---|
| Details tab | |
| Number | Number of the self-attestation record. This field is auto-filled. |
| Name | Unique name for the self-attestation record. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Self attestation form (continued)**

| Field | Description |
|---|---|
| Description | Helpful information about the self-attestation record. |
| Attestation template | Default attestation template that is provided with the base system and that is used for creating the self-attestation. The name of the template is *Operational Resilience Attestation Template*. |
| PDF template | Default PDF Template that is provided with the base system to export an attestation to a PDF. The name of the template is *Default Self Attestation HTML Template*. |
| Signature | Field to attach the signature image with the attestation. Select the e-signature that you can embed in the template.<br>**Note:** You must select the supported file format, such as either the JPEG, PNG, BMP, GIF, ICO, SVG format, for the signature image. |
| Assignees panel | |
| Owner | Label for the self-attestation record that is displayed in the UI. This field is auto-filled. |
| Milestones panel | |
| Attestation due date | Date on which the attestation is due. |
| Attested date | Date and time when the attestation is certified. |
| Compose panel | |
| Additional comments (Customer visible) | Extra comments for the self-attestation. This field is auto-filled. |
| Work notes (Private) | Work notes for the self-attestation. This field is auto-filled. |
| Activity | Activities that are associated with the self-attestation. |
| Attachments | Attachments that are available with the self-attestation, such as the PDF of the self-attestation. You can download, rename, or remove the PDF from the form. |
| Services tab (This tab is displayed after you add a service to the attestation.) | |
| Name | Name of the business service. |
| Owned by | Owner of the business service. |
| Business criticality | Business criticality of the service. |
| Assessment tab (This tab is displayed after you submit the attestation.) | |
| Operational Resilience Attestation Template | Assessment questionnaire for the services. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Self attestation form (continued)**

| Field | Description |
|---|---|
| | **Note:** If you're the owner of the attestation, you can view the assessment. You can fill in the responses to the questions and submit the assessment for the self-attestation. |

### Submit a self-attestation to certify the status of the services

Submit a self-attestation in Operational Resilience Workspace so that you can certify the status of the services and generate a PDF of the self-attestation report for your records.

## Before you begin

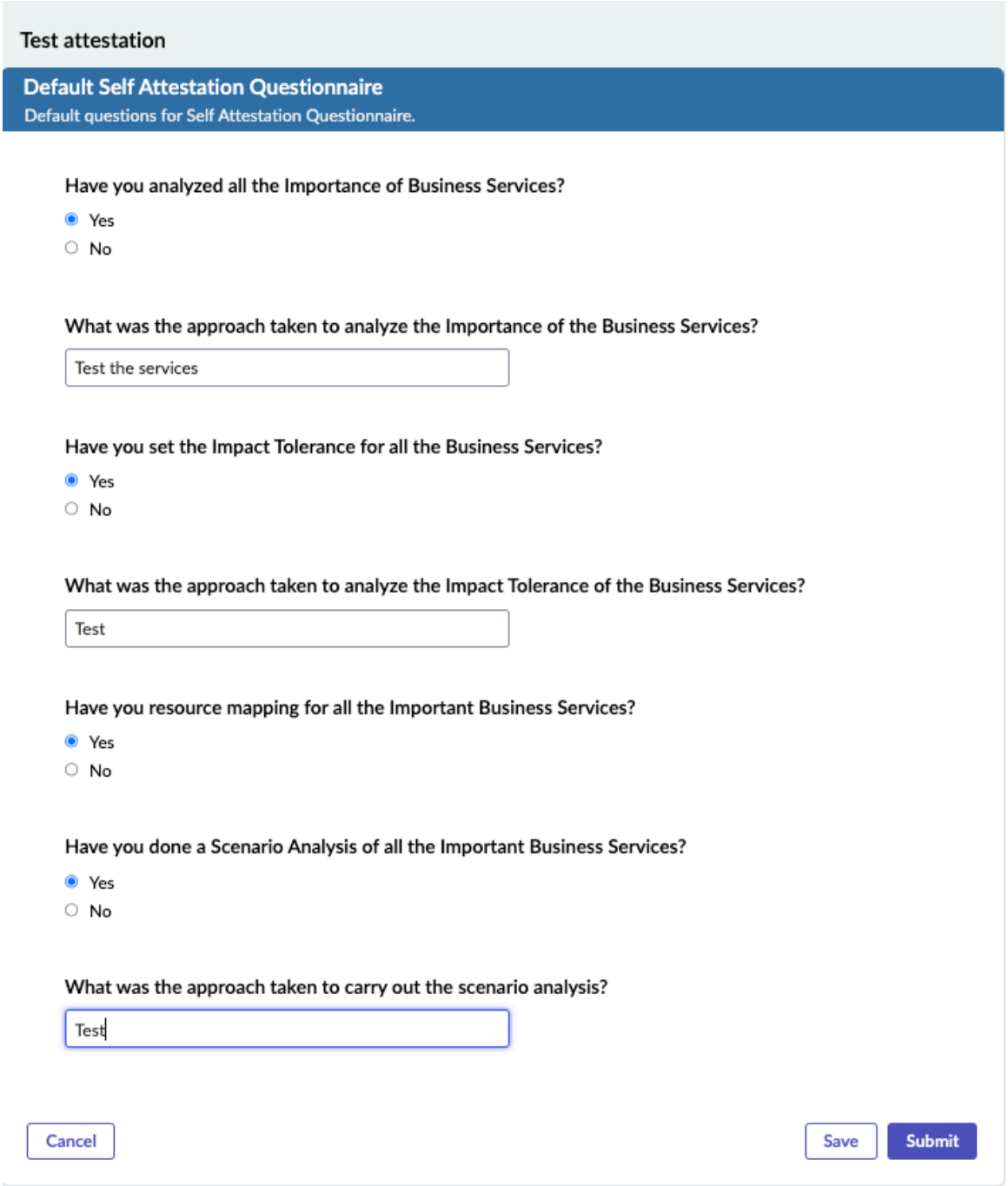
Role required: sn_oper_res.manager

## Procedure

1. Navigate to **All** > **Operational Resilience Workspace** > **Self attestations** and select the self-attestation that you're working on.
2. In the **Assessment** tab, respond to the questions in the assessment.
   In the **Assessment** tab, an assessment questionnaire for the services is displayed. As an assessor, you can respond to the questions in the assessment as shown in the following examples.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Importance and Impact Tolerance Assessment Template-page-1



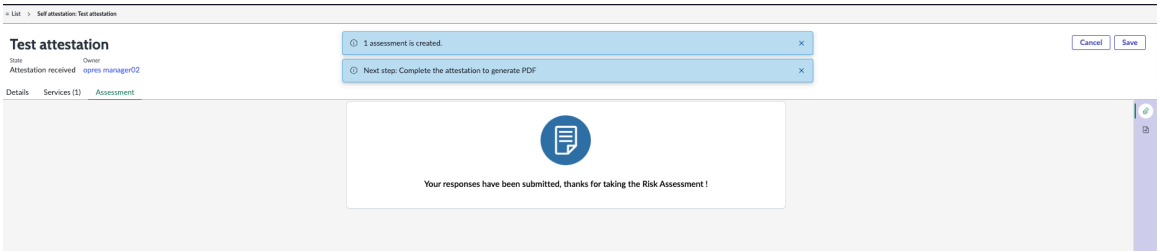

3. Click **Submit**.
   When you submit the assessment, your responses are stored in the application.

   The following informational message is displayed on the screen: *Your responses have been submitted. Thanks for taking the Risk Assessment..*

   You've updated the state of the self-attestation to **Attestation received** as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

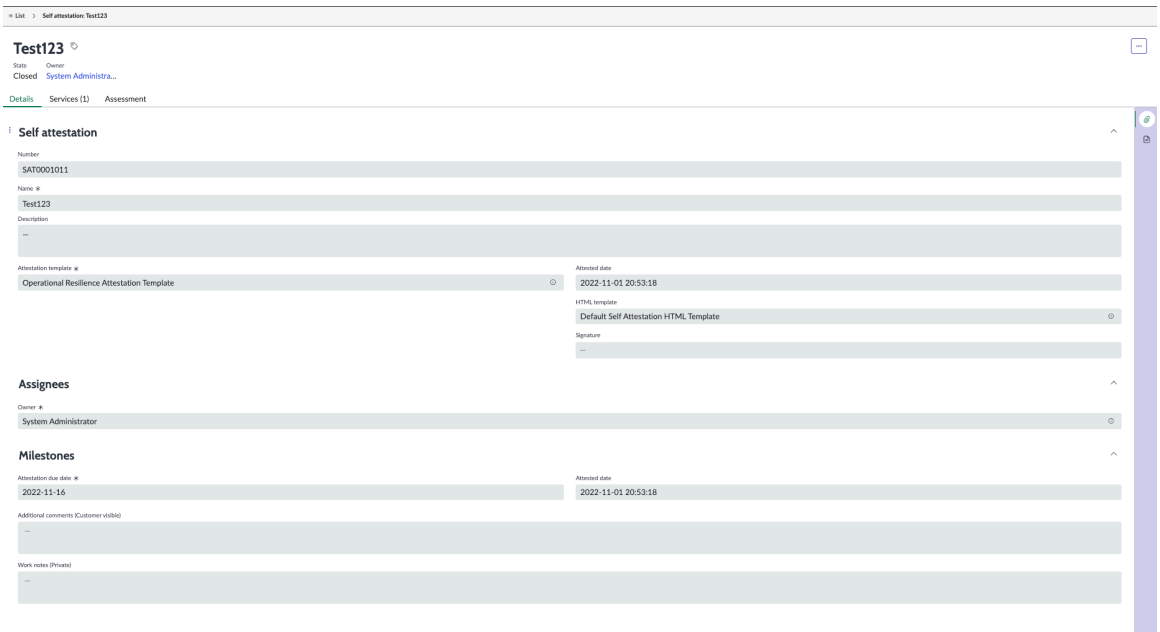
**Attestation received**




4. Click **Save**.
   Your responses to the assessment are saved in the application.
5. Click **Export to PDF**.
   You can export a copy of the answers in the PDF format.
   The following informational message is displayed on the screen: *PDF has been successfully generated for download. You can download the PDF in the activity section.*
6. Click **Save**.
   Your responses are stored in the application.
   The PDF of the self-attestation report is displayed in the Activity section in the self-attestation form.
7. Click **Close**.
   By performing this action, you can close the self-attestation.

   You've updated the state of the self-attestation to **Closed** as shown in the following example.

**Attestation closed**




## Associating an issue in Operational Resilience Workspace

You can associate an issue with multiple objects such as controls, control objectives, risks, and so on in Operational Resilience Workspace. You can add an existing issue or create an issue for a given business service or a scenario analysis in the Operational Resilience application.

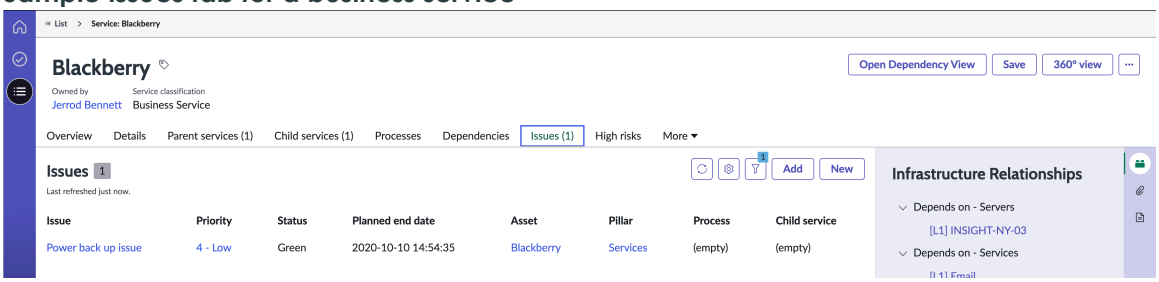
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Issues are used to capture the current problems or gaps that have been observed in the application environment. You can also track a plan of action to remediate the gaps.

With the new issue architecture, you can associate an existing issue with the controls or risks. You can also create an issue where you can now specify one or multiple controls, control objectives, risks, risk statements, citations, and so on, that are impacted by the issue.

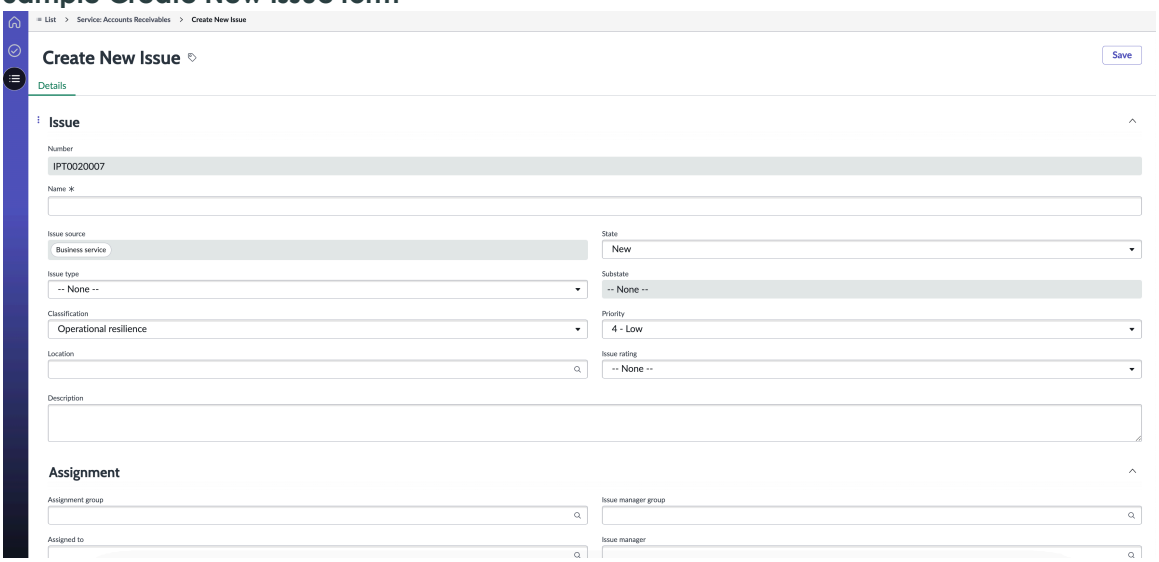
In Operational Resilience, you can add an existing issue or create an issue for a given business service or a scenario analysis. A sample **Issues** tab for a business service is shown in the following example.

### Sample Issues tab for a business service




When you select **New** on the **Issues** tab to create an issue for a business service or a scenario analysis, the Create New Issue form is displayed as shown in the following example.

### Sample Create New Issue form




For the descriptions of the field values on the Create New Issue form, see Create New Issue form.

### Create New Issue form

Use the Create New Issue form in Operational Resilience Workspace to add an issue to a business service or a scenario analysis.

## Create New Issue form

For a description of the field values, see the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create New Issue form

| Field | Description |
|---|---|
| Issue | |
| Number | Number of the issue. This field is auto-filled. |
| Name | Name of the issue. |
| Issue source | Source of the issue, such as Business service or Scenario analysis. This field is auto-filled. |
| Issue type | Source from where the issue was created. This field is auto-populated with one of the following options based on how the issue is created:<br>• Control design effectiveness failure<br>• Control operative effectiveness failure<br>• Control does not meet requirement<br>• Control does not exist<br>• Non-compliance to a regulation<br>• Non-compliance to a policy<br>• Improvement or suggestion to an existing policy<br>• Recommendation for a new policy<br>• process optimization or improvement<br>• Observation<br>• Data breach<br>• Fraud<br>• Misstatement<br>• Training<br>• Documentation |
| Classification | Classification of the issue. This field is auto-populated with one of the following options:<br>• Audit<br>• Compliance<br>• Operational Resilience<br>• Risk<br>• Vendor |
| Location | Location of the issue. |
| State | State of the issue. Available options are:<br>• New<br>• Analyze<br>• Respond<br>• Review |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| | • Closed Complete<br>• Closed Incomplete |
| Substate | Substate of the issue. This field is auto-filled. |
| Priority | Priority of the issue. Available options are:<br>• Critical<br>• High<br>• Moderate<br>• Low<br>• Planning |
| Issue rating | Rating of the issue. Available options are:<br>• Very High<br>• High<br>• Moderate<br>• Low<br>• Very Low |
| Description | Approver of the scenario analysis plan. |
| Assignment | |
| Assignment group | Assignment group for the issue. For example, Application Development group. |
| Assigned to | User that the issue is assigned to. |
| Issue manager group | Manager group that the issue is assigned to. Available options are:<br>• Compliance Managers<br>• IT Risk Managers<br>• Risk Managers |
| Issue manager | Manager that the issue is assigned to. |
| Watchlist | Users who are on the watchlist for the issue. |
| Schedule | |
| Due date | Date when the issue is due. |
| Confirmed date | Confirmation date for the issue. This field is auto-filled. |
| Planned start date | Planned start date for the issue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| Planned end date | Planned end date for the issue. |
| Duration | Duration for the issue in days, hours, minutes, and seconds. |
| Created | Date on which the issue is created. This field is auto-filled. |
| Closed | Date on which the issue is closed. |
| Actual start date | Actual start date for the issue. |
| Actual end date | Actual end date for the issue. |
| Actual duration | Actual duration for the issue in days, hours, minutes, and seconds. |
| Issue grouping | |
| Parent issue | Parent issue that is associated with the issue. |
| Issue group rule | Group rule for the issue. This field is auto-filled. |
| Action plan | |
| Recommendation | Recommendation for the issue. |
| Action plan | Action plan for the issue. |
| Activity | |
| Work notes | Work notes for the issue. |
| Additional comments | Additional comments for the issue. |
| Settings | |
| Functional domain | Functional domain that the issue belongs to. For example, an issue may belong to the IT Risk and Compliance domain. |

## Displaying reports in Operational Resilience

Operational Resilience allows an organization to continue to provide business services in the face of adverse operational events, such as fire, pandemic, extreme weather, or hacking. By anticipating, preventing, recovering from, and adapting to these events, the dashboard provides a clear understanding of your company's operational resilience.

### Displaying reports for different user roles

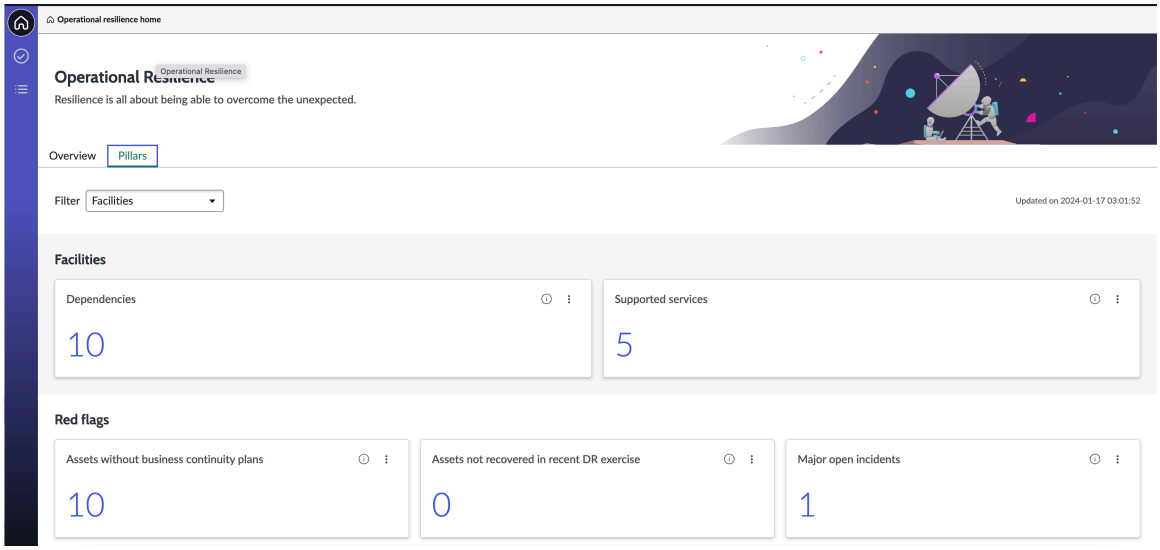
The Home page in the Operational Resilience Workspace displays separate reports for BCM Professional and IRM Professional.

### Roles for accessing the reports

Users with the following roles can access the BCM reports in the Operational Resilience Workspace as shown in the example.

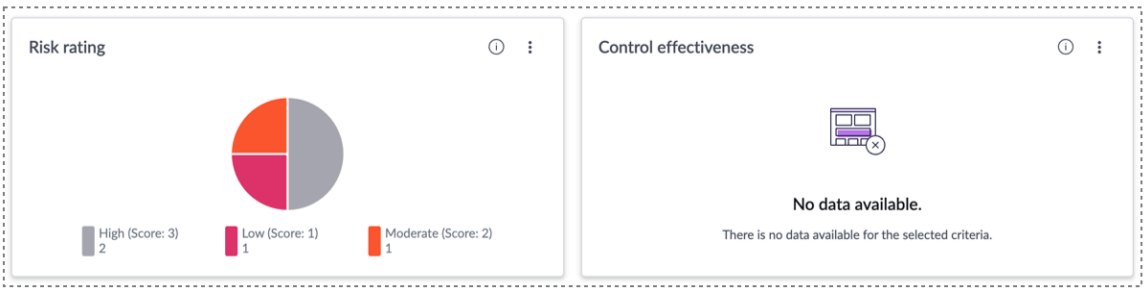
- sn_oper_res.bcm_opres_admin
- sn_oper_res.bcm_opres_manager
- sn_oper_res.bcm_opres_user

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




Users with the following roles can access the IRM reports in the Operational Resilience Workspace as shown in the example.

- sn_oper_res.irm_opres_admin
- sn_oper_res.irm_opres_manager
- sn_oper_res.irm_opres_user




## Use cases for using the dashboard

For examples of how different people in your organization would use this dashboard, see the following use cases.

| User | Dashboard use |
| --- | --- |
| Operational Resilience Manager and Operational Resilience User | Use the dashboards and reports to ensure operational resilience in the organization.<br><br>The Operational Resilience Manager also uses the reports to follow up with the respective owners in the areas of risks, control failures, open overdue Priority 1 issues, assets with incidents, assets with vulnerabilities, and entities that do not have continuity or recovery plans. |

For more information, see Roles installed with Operational Resilience.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Data visualizations

The GRC: Operational Resilience dashboard contains the following visualizations:

### Reports on the Overview tab

| Title | Type | Description |
|---|---|---|
| Services | Single Score | The number of critical services delivered to your customers.<br><br>Source table for this report: Entity to Entity Type [sn_grc_m2m_profile_profile_type] |
| Assets | Single Score | The number of critical entities that are supporting the services delivered to your customers.<br><br>Source table for this report: Critical Entities [sn_oper_res_profile] |
| Service Outages | Single Score | The number of critical services reporting a service outage.<br><br>Source table for this report: Critical Service Outage [sn_oper_res_critical_service_outage] |
| Services with High Risks | Single Score | Services in each of the pillars identified as being high risk.<br><br>The data in this report is pulled from the Advanced Risk Assessment application.<br><br>Source table for this report: Services with High Risks [sn_oper_res_risk] |
| Services with Failed Controls | Single Score | Services in each of the pillars identified as being impacted by failed controls.<br><br>The data in this report is pulled from the Policy and Compliance Management application.<br><br>Source table for this report: Services with Failed Controls [sn_oper_res_failed_control] |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Reports on the Overview tab (continued)**

| Title | Type | Description |
|---|---|---|
| Degraded Services | Single Score | The number of critical services reporting a degraded level of service.<br><br>Source table for this report: Critical Service Outage [sn_oper_res_critical_service_outage] |
| Services with High Risks | Trend Report | Services in each of the pillars identified as being high risk.<br><br>The data in this report is pulled from the Advanced Risk Assessment application.<br><br>Source table for this report: Services with High Risks [sn_oper_res_risk] |
| Services with Failed Controls | Trend Report | Services in each of the pillars identified as being impacted by failed controls.<br><br>The data in this report is pulled from the Policy and Compliance Management application.<br><br>Source table for this report: Services with Failed Controls [sn_oper_res_failed_control] |
| Services with Overdue Issues | Trend Report | Services impacted by stress tests performed using scenario analysis. The report shows services that have failed or breached their defined thresholds.<br><br>The report shows the number of P1 issues in each of the pillars that are overdue.<br><br>Source table for this report: Services with Priority 1 Issues [sn_oper_res_issue] |
| Services with No BC/DR Plans | Trend Report | Services that have no Business Continuity or Disaster Recovery plans.<br><br>The data in this report is pulled from the Business |

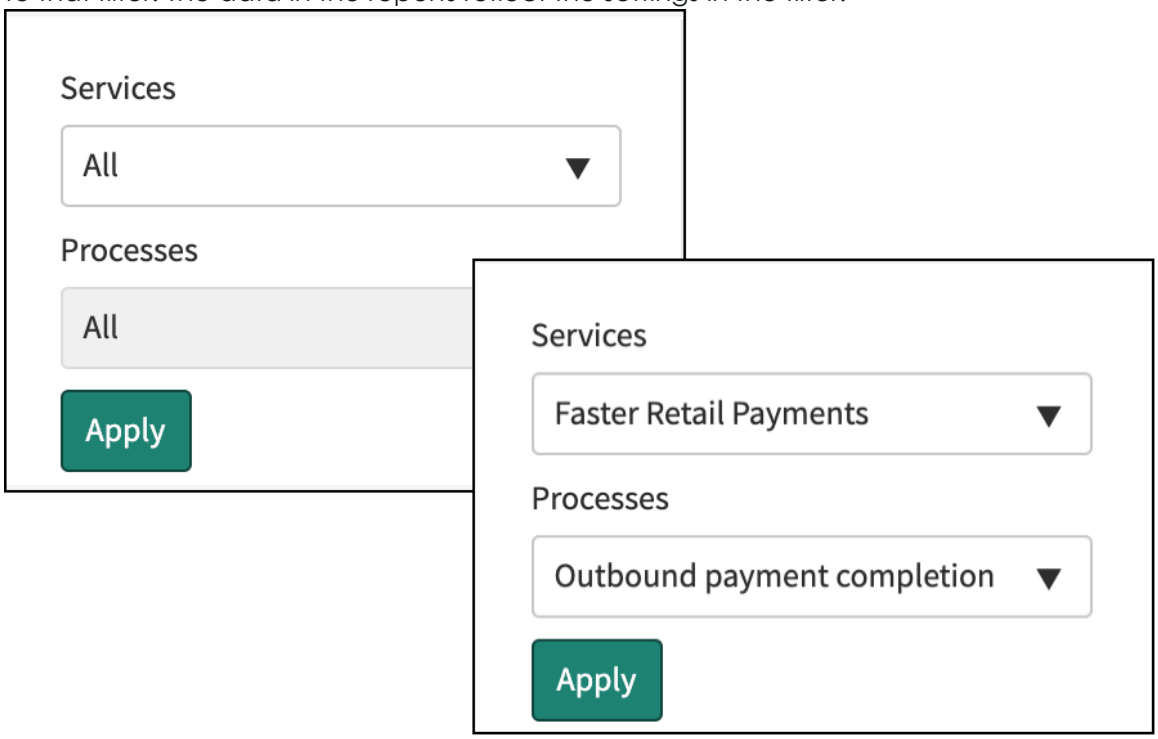
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Reports on the Overview tab (continued)**

| Title | Type | Description |
|---|---|---|
| | | Continuity Management application.<br><br>**Note:** If the Business Continuity Management application is not installed, this report will not have data.<br><br>Source table for this report: Business Continuity Plan [sn_oper_res_bcm_plan] |
| Top Risks to be Mitigated | Horizontal Bar | The top risks threatening your organization compared with your impacted services. This report can be useful for determining where to start your mitigation efforts and in what areas you should devote the most resources around implementing controls.<br><br>Source table for this report: Services with High Risks [sn_oper_res_risk] |
| Top Controls to be Strengthened | Horizontal Bar | The failing controls that impact the most critical services.<br><br>Source table for this report: Services with Failed Controls [sn_oper_res_failed_control] |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** The **Service Details** tab includes a filter that you can use to view all services and processes used by your organization, or you can drill down into a particular report to view information specific to that filter. The data in the reports reflect the settings in the filter.




### Visualizations on the Service Details tab

| Title | Type | Description |
|---|---|---|
| Critical Entities | Single Score | The number of critical entities that are supporting the filtered service and process.<br><br>Source table for this report: Critical Entities [sn_oper_res_profile] |
| High Risks | Single Score | The number of high risk services identified in the filtered service and process.<br><br>The data in this report is pulled from the Advanced Risk Assessment application.<br><br>Source table for this report: Services with High Risks [sn_oper_res_risk] |
| Failed Controls | Single Score | The number of failed controls identified in the filtered service and process.<br><br>The data in this report is pulled from the Policy and |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Visualizations on the Service Details tab (continued)**

| Title | Type | Description |
|---|---|---|
| | | Compliance Management application.<br><br>Source table for this report: Services with Failed Controls [sn_oper_res_failed_control] |
| High Risks | Trend Report | A trend report of high risk services by pillar identified in the filtered service and process.<br><br>The data in this report is pulled from the Advanced Risk Assessment application.<br><br>Source table for this report: Services with High Risks [sn_oper_res_risk] |
| Failed Controls | Trend Report | A trend report of failed controls by pillar identified in the filtered service and process.<br><br>The data in this report is pulled from the Policy and Compliance Management application.<br><br>Source table for this report: Services with Failed Controls [sn_oper_res_failed_control] |
| Overdue P1 Issues | Trend Report | A trend report of overdue P1 issues by pillar identified in the filtered service and process.<br><br>The data in this report shows the number of P1 issues in each of the pillars that are overdue.<br><br>Source table for this report: Services with Priority 1 Issues [sn_oper_res_issue] |
| Entities with Failed BC/DR Plans | Trend Report | A trend report of entities with objects that have Business Continuity or Disaster Recovery plans, but for which the plans are failing. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Visualizations on the Service Details tab (continued)

| Title | Type | Description |
|---|---|---|
| | | The data in this report is pulled from the Business Continuity Management application.<br><br>**Note:** If the Business Continuity Management application is not installed, this report will not have data.<br><br>Source table for this report: Business Continuity Plan [sn_oper_res_bcm_plan] |

### Visualizations on the Technology tab

| Title | Type | Description |
|---|---|---|
| Critical Assets | Single Score | The number of critical assets, such as business applications or any of the underlying infrastructure that allows business users to work, being managed by the technology team.<br><br>Source table for this report: Critical Entities [sn_oper_res_profile] |
| Supported Services | Single Score | The number of critical business services being managed by the team.<br><br>Source table for this report: Critical Entities [sn_oper_res_profile] |
| Major Open Incidents | Single Score | The number of critical assets that have incidents opened against them.<br><br>Source table for this report: Critical Service Incident [sn_oper_res_incident] |
| Assets without Plans | Single Score | The number of critical assets that do not have an associated disaster recovery plan implemented. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Visualizations on the Technology tab (continued)

| Title | Type | Description |
|---|---|---|
| | | Source table for this report: Business Continuity Plan [sn_oper_res_bcm_plan] |
| Assets with Failed Tests | Single Score | The number of critical assets that have disaster recovery plans, but the plans have failed.<br><br>Source table for this report: Business Continuity Plan [sn_oper_res_bcm_plan] |
| Assets Risk Rating | Donut Report | |
| Assets Control Effectiveness | The risk assessments associated with technology assets that have a residual risk. Residual risks can be defined in the qualitative rating criteria for the Residual risk assessment type.<br><br>The data in this report is pulled from the Advanced Risk Assessment application.<br><br>Source table for this report: Risk Assessment [sn_risk_advanced_risk_assessment_instance | |
| Assets Issues | The controls for assets that are compliant and non-compliant. The report also shows the number of controls that have not yet been attested.<br><br>Source table for this report: Control [sn_compliance_control] | The number of critical, high, moderate, and low technology-related issues that have been opened for the critical assets or controls.<br><br>Source table for this report: Issue [sn_grc_issue] |
| Top Risks to be Mitigated | Horizontal Bar | The top technology risks threatening your impacted assets. This report can be useful for determining where to start your mitigation efforts and in what areas you should devote the most resources around implementing controls. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Visualizations on the Technology tab (continued)

| Title | Type | Description |
|---|---|---|
| | | Source table for this report: Services with High Risks [sn_oper_res_risk] |
| Top Controls to be Strengthened | Horizontal Bar | The failing controls that impact the most critical services.<br><br>Source table for this report: Services with Failed Controls [sn_oper_res_failed_control] |
| Top Vulnerabilities to be Fixed | Horizontal Bar | The top vulnerable controls that are affecting technology assets, such as web applications, compared with impacted assets.<br><br>The data in this report is pulled from the Vulnerability Response application. If Vulnerability Response is not installed, this report will be blank.<br><br>Source table for this report: Vulnerable Entities [sn_oper_res_vul_profile]<br><br>**Note:** The Vulnerability Response application is used only for the technical services. |

### Visualizations on the Facilities tab

| Title | Type | Description |
|---|---|---|
| Critical Facilities | Single Score | The number of critical facilities used by business users being managed by the facilities team.<br><br>Source table for this report: Critical Entities [sn_oper_res_profile] |
| Supported Services | Single Score | The number of critical business services being managed by the team. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Visualizations on the Facilities tab (continued)

| Title | Type | Description |
|---|---|---|
| | | Source table for this report: Critical Entities [sn_oper_res_profile] |
| Current Incidents | Single Score | The number of critical facilities that have incidents opened against them.<br><br>Source table for this report: Critical Service Incident [sn_oper_res_incident] |
| Facilities without Plans | Single Score | The number of critical facilities that do not have an associated disaster recovery plan implemented.<br><br>Source table for this report: Business Continuity Plan [sn_oper_res_bcm_plan] |
| Facilities with Failed Tests | Single Score | The number of critical facilities that have disaster recovery plans, but the plans have failed.<br><br>Source table for this report: Business Continuity Plan [sn_oper_res_bcm_plan] |
| Facilities Risk Rating | Donut Report | The risk assessments associated with facilities that have a residual risk. Residual risks can be defined in the qualitative rating criteria for the Residual risk assessment type.<br><br>Source table for this report: Risk Assessment [sn_risk_advanced_risk_assessment_instance] |
| Facilities Control Effectiveness | Donut Report | The controls for facilities that are compliant and non-compliant. The report also shows the number of controls that have not yet been attested.<br><br>Source table for this report: Control [sn_compliance_control] |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Visualizations on the Facilities tab (continued)

| Title | Type | Description |
|---|---|---|
| Facilities Issue Priority | Donut Report | The number of critical, high, moderate, and low issues that have been opened for the critical facilities.<br><br>Source table for this report: Issue [sn_grc_issue] |
| Top Risks to be Mitigated | Horizontal Bar | The top risks threatening your impacted facilities. This report can be useful for determining where to start your mitigation efforts and in what areas you should devote the most resources around implementing controls.<br><br>Source table for this report: Services with High Risks [sn_oper_res_risk] |
| Top Controls to be Strengthened | Horizontal Bar | The failing controls that impact the most critical services.<br><br>Source table for this report: Services with Failed Controls [sn_oper_res_failed_control] |

### Visualizations on the People tab

| Title | Type | Description |
|---|---|---|
| Critical Organizations | Single Score | The number of critical organizations used by business users being managed by the human resources team.<br><br>Source table for this report: Critical Entities [sn_oper_res_profile] |
| Supported Services | Single Score | The number of critical business services being managed by the team.<br><br>Source table for this report: Critical Entities [sn_oper_res_profile] |
| Organizations without Plans | Single Score | The number of critical organizations that do not |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Visualizations on the People tab (continued)**

| Title | Type | Description |
|---|---|---|
| | | have an associated disaster recovery plan implemented.<br><br>Source table for this report: Business Continuity Plan [sn_oper_res_bcm_plan] |
| Organizations with Failed Tests | Single Score | The number of critical organizations that have disaster recovery plans, but the plans have failed.<br><br>Source table for this report: Business Continuity Plan [sn_oper_res_bcm_plan] |
| Organizations Risk Rating | Donut Report | The risk assessments associated with organizations that have a residual risk. Residual risks can be defined in the qualitative rating criteria for the Residual risk assessment type.<br><br>Source table for this report: Risk Assessment [sn_risk_advanced_risk_assessment_instance] |
| Organizations Control Effectiveness | Donut Report | The controls for organizations that are compliant and non-compliant. The report also shows the number of controls that have not yet been attested.<br><br>Source table for this report: Control [sn_compliance_control] |
| Organizations Issue Priority | Donut Report | The number of critical, high, moderate, and low issues that have been opened for the critical organizations.<br><br>Source table for this report: Issue [sn_grc_issue] |
| Top Risks to be Mitigated | Horizontal Bar | The top risks threatening your impacted organizations. This report can be useful for determining where to start your mitigation efforts and in what areas you should devote the most resources |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Visualizations on the People tab (continued)

| Title | Type | Description |
|---|---|---|
| | | around implementing controls.<br><br>Source table for this report: Services with High Risks [sn_oper_res_risk] |
| Top Controls to be Strengthened | Horizontal Bar | The failing controls that impact the most critical services.<br><br>Source table for this report: Services with Failed Controls [sn_oper_res_failed_control] |

### Visualizations on the Suppliers tab

| Title | Type | Description |
|---|---|---|
| Critical Suppliers | Single Score | The number of critical suppliers used by business users.<br><br>Source table for this report: Critical Entities [sn_oper_res_profile] |
| Supported Services | Single Score | The number of critical business services being managed by the team.<br><br>Source table for this report: Critical Entities [sn_oper_res_profile] |
| Suppliers without Plans | Single Score | The number of critical organizations that do not have an associated disaster recovery plan or supply chain plan implemented.<br><br>Source table for this report: Business Continuity Plan [sn_oper_res_bcm_plan] |
| Suppliers with Failed Tests | Single Score | The number of critical suppliers that have disaster recovery plans, but the plans have failed.<br><br>Source table for this report: Business Continuity Plan [sn_oper_res_bcm_plan] |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Visualizations on the Suppliers tab (continued)**

| Title | Type | Description |
|---|---|---|
| Suppliers Risk Rating | Donut Report | The critical, high, moderate, and low risks associated with the suppliers.<br><br>Source table for this report: Risk Assessment [sn_risk_advanced_risk_assessment_instance] |
| Suppliers Control Effectiveness | Donut Report | The controls for suppliers that are compliant and non-compliant. The report also shows the number of controls that have not yet been attested.<br><br>Source table for this report: Control [sn_compliance_control] |
| Suppliers Issue Priority | Donut Report | The number of critical, high, moderate, and low issues that have been opened for the critical suppliers.<br><br>Source table for this report: Issue [sn_grc_issue] |
| Top Risks to be Mitigated | Horizontal Bar | The top risks threatening your impacted suppliers. This report can be useful for determining where to start your mitigation efforts and in what areas you should devote the most resources around implementing controls.<br><br>Source table for this report: Services with High Risks [sn_oper_res_risk] |
| Top Controls to be Strengthened | Horizontal Bar | The failing controls that impact the most critical services.<br><br>Source table for this report: Services with Failed Controls [sn_oper_res_failed_control] |

## Operational Resilience reference

Reference topics provide additional information such as tables, roles, and properties that are installed with the Operational Resilience application. Several types of components are

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

installed with the activation of the Operational Resilience application, including properties, roles, and tables.

## Components installed with Operational Resilience

Several types of components are installed with the activation of the Operational Resilience application, including tables, user roles, and scheduled jobs.

### Properties installed with Operational Resilience

When you install the Operational Resilience application, several system properties are added to your instance. You may not need to modify these properties. The user with the sn_oper_res.admin role can maintain these properties.

## Properties installed

| Property | Description |
|---|---|
| sn_oper_res.critical_services | sys_id of the service entity type.<br>**Type**: string |
| sn_oper_res.critical_business_processes | sys_id of the business process entity type.<br>**Type**: string |
| sn_oper_res.business_process_pillar | sys_id of the Process pillar.<br>**Type**: string |
| sn_oper_res.max_top | Number of vulnerabilities to be displayed in the **Top vulnerabilities to be fixed** report in the Operational Resilience dashboard.<br>• **Type**: integer<br>• **Default value**: 5 |
| sn_oper_res.useAdvancedRisk | Computation, if true, that is based on the Advanced Risk application. If false, the computation is based on the Risk Management application.<br>• **Type**: True or false<br>• **Default value**: true |

### Roles installed with Operational Resilience

Several types of roles are installed with the Operational Resilience application.

## Roles that are installed with Operational Resilience

Beginning with the Utah release, two set of new roles are added for BCM Professional and IRM Professional.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** For more information on roles and FAQs, see KB0555605.

**Model types when Lite Apps are installed**

| Roles | Family | Comments |
|---|---|---|
| sn_oper_res.admin | IRM | None |
| sn_oper_res.manager | IRM | None |
| sn_oper_res.user | IRM | The sn_oper_res.user role is required to access Vulnerability profile records. |
| New roles introduced | | |
| sn_oper_res.bcm_opres_admin | BCM | The sn_bcm.viewer role is required to access the BCM Configurable Workspace workspace.<br><br>A user with the sn_oper_res.bcm_opres_user + role can access both Operational Resilience Workspace and BCM Configurable Workspace. |
| sn_oper_res.bcm_opres_manager | BCM | |
| sn_oper_res.bcm_opres_user | BCM | |
| sn_oper_res.irm_opres_admin | IRM | A user with the sn_oper_res.irm_opres_user + role can access the Operational Resilience Workspace, but cannot access the Compliance Workspace and Risk Workspace.<br><br>Extra roles are needed to access the Compliance Workspace and Risk Workspace. |
| sn_oper_res.irm_opres_manager | IRM | |
| sn_oper_res.irm_opres_user | IRM | |

## Roles created for BCM Professional and IRM Professional

- The following roles are created for the BCM Professional users:

  **Note:** When the app-grc-bcm-lite applications are not installed, the users with these roles are counted as operators.

  - sn_oper_res.bcm_opres_admin
  - sn_oper_res.bcm_opres_manager
  - sn_oper_res.bcm_opres_user
- The following roles are created for the IRM Professional users:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** When the app-grc-bcm-lite applications are not installed, the users with these roles are counted as operators.

  - sn_oper_res.irm_opres_admin
  - sn_oper_res.irm_opres_manager
  - sn_oper_res.irm_opres_user
- When the following Lite applications are installed, the users with the sn_oper_res.bcm_opres_user, sn_oper_res.irm_opres_user, or sn_oper_res.user roles are counted as Lite operators.
  - BCM Lite application: app-grc-bcm-lite (Plugin id: com.snc.app_grc_bcm_lite)
  - IRM Lite application: app-grc-business-user-lite (Plugin id: com.sn_grc_lite)
- The sn_oper_res.admin, sn_oper_res.manager, and sn_oper_res.user roles are included in IRM.

## Roles required for accessing the Workspaces

A user with one of the following roles can access the Operational Resilience Workspace and BCM Configurable Workspace:

- sn_oper_res.bcm_opres_user
- sn_oper_res.bcm_opres_manager
- sn_oper_res.bcm_opres_admin

A user with any role below can access the Operational Resilience Workspace:

- sn_oper_res.irm_opres_user
- sn_oper_res.irm_opres_manager
- sn_oper_res.irm_opres_admin

A user with one of the following roles can access the Risk Workspace:

- sn_risk_workspace.business_op_risk_manager
- sn_risk_workspace.IT_risk_manager
- sn_risk_workspace.operatonal_risk_manager

A user with one of the following roles can access the Compliance Workspace:

- sn_compliance_ws.corporate_compliance_analyst
- sn_compliance_ws.corporate_compliance_manager
- sn_compliance_ws.it_compliance_manager

### Roles installed with Operational Resilience

| Role name | Description |
|---|---|
| Operational Resilience administrator<br><br>[sn_oper_res.admin] | The Operational Resilience administrator is responsible for: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed with Operational Resilience (continued)**

| Role name | Description |
|---|---|
| | • Configuring scenarios<br>• Setting up entity types, entity filters, and reporting pillars based on dashboard requests from the business teams.<br>• Customizing reports on the Operational Resilience dashboard.<br><br>The Operational Resilience administrator should have the ITIL role to add the CMDB relationship between the service and the process.<br><br>The Operational Resilience administrator role contains the following roles:<br>• sn_grc.admin<br>• sn_oper_res.manager |
| Operational Resilience Manager<br><br>[sn_oper_res.manager] | The Operational Resilience Manager is responsible for:<br>• Ensuring operational resilience in the organization using the dashboards and reports<br>• Reviewing reports on the Operational Resilience dashboard, as well as supporting data.<br><br>The Operational Resilience Manager role contains the following roles:<br>• sn_grc.manager<br>• sn_compliance.reader<br>• sn_oper_res.user<br>• sn_risk.reader |
| Operational Resilience User<br><br>[sn_oper_res.user] | The Operational Resilience User is responsible for:<br>• Reviewing reports on the Operational Resilience dashboard, as well as supporting data.<br>• Completing impact tolerance and test plans for individuals assigned to the service impact analysis.<br><br>The Operational Resilience User can access the Vulnerability Response data.<br><br>The Operational Resilience User role contains the following roles: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed with Operational Resilience (continued)**

| Role name | Description |
|---|---|
| | • sn_incident.read<br>• sn_grc.reader<br>• task_editor |
| BCM and Operational Resilience Administrator [sn_oper_res.bcm_opres_admin] | The BCM and Operational Resilience Administrator role contains the following roles:<br>• sn_oper_res.bcm_opres_manager<br>• sn_oper_res.admin |
| BCM and Operational Resilience Manager [sn_oper_res.bcm_opres_manager] | The BCM and Operational Resilience Manager role contains the following roles:<br>• sn_oper_res.bcm_opres_user<br>• sn_oper_res.manager |
| BCM and Operational Resilience User [sn_oper_res.bcm_opres_user] | The BCM and Operational Resilience User role has the following permissions:<br>• Can read the BCM UIB Workspace.<br>• Cannot access the IRM reports or data.<br><br>The BCM and Operational Resilience User role contains the following roles:<br>• sn_bcm.viewer<br>• sn_oper_res.user |
| IRM Operational Resilience User [sn_oper_res.irm_opres_user] | The IRM Operational Resilience User role cannot access the BCM reports and data. It contains:<br>• sn_grc.reader<br>• sn_oper_res.user<br><br>The following user roles are contained only when policy and compliance management and risk management are installed:<br>• sn_compliance.reader<br>• sn_risk.reader |
| IRM Operational Resilience Administrator [sn_oper_res.irm_opres_admin] | The IRM Operational Resilience Administrator role contains the following roles:<br>• sn_oper_res.irm_opres_manager<br>• sn_oper_res.admin |

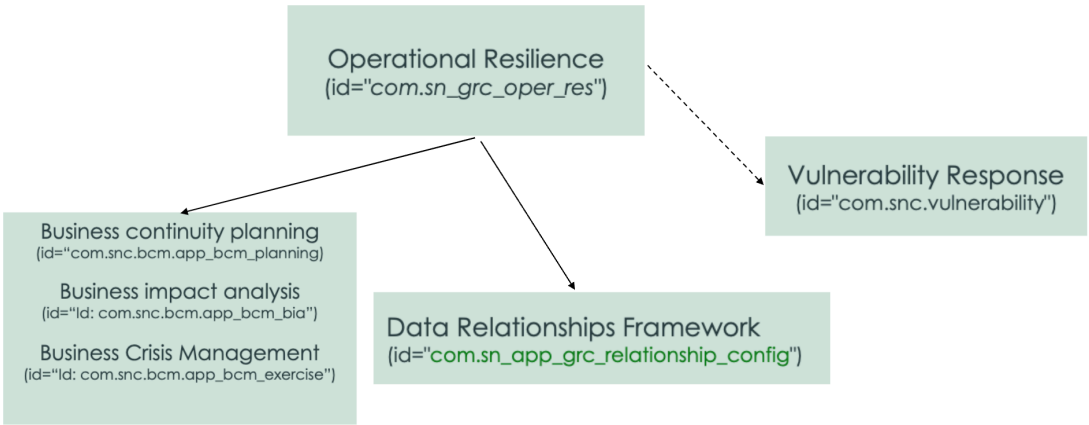
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed with Operational Resilience (continued)**

| Role name | Description |
|---|---|
| IRM Operational Resilience Manager [sn_oper_res.irm_opres_manager] | The IRM Operational Resilience Manager role contains the following roles:<br>• sn_oper_res.irm_opres_user<br>• sn_oper_res.manager |

## Plugin dependencies for BCM Professional

For BCM Professional, the following mandatory applications are installed with Operational



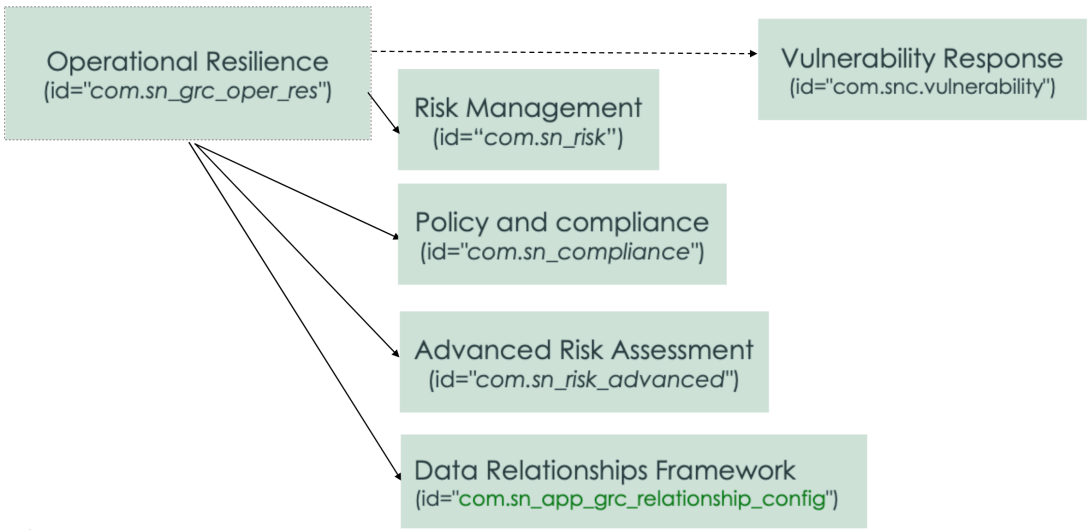

Resilience.

- Business Continuity Planning (com.snc.bcm.app_bcm_planning)
- Business Impact Analysis (com.snc.bcm.app_bcm_bia)
- Crisis Management (com.snc.bcm.app_bcm_exercise)
- Data Relationships Framework (com.sn_app_grc_relationship_config)
- Optional: Vulnerability Response (com.snc.vulnerability)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Plugin dependencies for IRM Professional

For IRM Professional, the following mandatory applications are installed with Operational




Resilience.

- Advanced Risk Assessment (com.sn_risk_advanced)
- Data Relationships Framework (com.sn_app_grc_relationship_config)
- Policy and Compliance Management (com.sn_compliance)
- Risk Management (com.sn_risk)
- Optional: Vulnerability Response (com.snc.vulnerability)

### Scheduled jobs installed with Operational Resilience

When you download the Operational Resilience application, the *Compute Operational Resilience Compliance* scheduled job is added to your instance. As a user with the sn_oper_res.admin role, you may find this information useful.

## Scheduled jobs installed with the Operational Resilience application

The following scheduled jobs are installed with the Operational Resilience application:

**Scheduled jobs installed with Operational Resilience**

| Scheduled job | Description |
|---|---|
| *Compute Operational Resilience Compliance* | Scheduled job that gathers data from different applications including such as GRC: Advanced Risk, GRC: Risk Management, and GRC: Policy and Compliance Management, BCM, CMDB, and Vulnerability Response to calculate supporting data for various reports.<br><br>The scheduled job runs once a day and removes all the data from the previous day before creating new supporting data for the reports. The job uses different conditions to retrieve the data from different sources and |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Scheduled jobs installed with Operational Resilience (continued)**

| Scheduled job | Description |
|---|---|
| | saves it to the Operational Resilience staging tables. |

### Script includes installed with Operational Resilience

When you download the Operational Resilience application, several script includes are added to your instance.

## Script includes installed

| Script-includes | Description |
|---|---|
| ImportanceAssessmentUtils | Contains the utility functions that are being used in the importance assessment workflow. |
| OperationalResilienceAjax | Client callable script include that handles the interaction between the client side and the service side. |
| OperationalResilienceConstants | Contains the constants that are required in different places in the application. |
| OperationalResilienceComputationBase | Contains the utility functions that are being used to fetch the data from different places in Operational Resilience and also to fetch all the issues that are related to a business service's entity or configuration item (CI). |
| OperResBusinessServiceUtilBase | Contains the utility functions for the related lists in the business service form. |
| OpResPdfGenerationUtil | Contains the utility functions used in the PDF template scripts. |
| OpResAssessmentUtils | Contains the utility functions used to generate importance ratings. |
| OpResConditions | Contains the utility functions for conditions. |
| RelatedListOpResIssueFilter | Contains the utility functions for the issues related list. |
| ScenarioAnalysisUtils | Contains the utility functions that are being used in the scenario analysis workflow. |
| SelfAttestationUtilsBase | Contains the utility functions that are being used in the Self-attestation workflow. |
| ScenarioAnalysisIssuesRLCandidateFilter | Contains the utility functions for the issues that are being used in a scenario analysis. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Tables installed with Operational Resilience

Several types of tables are installed with the Operational Resilience application.

## Tables installed

**Tables installed with Operational Resilience**

| Table name | Description |
|---|---|
| Activity log (sn_oper_res_activity_log) | Activity log for the application. |
| ASMT rating scale (sn_oper_res_asmt_rating_scale) | ASMT rating scale. |
| BCM plan (sn_oper_res_bcm_plan) | BCM plan. |
| Choice (sn_grc_choice) | List of all GRC choices. |
| Change request (sn_oper_res_change_request) | Change request created for the application. |
| Critical service outage (sn_oper_res_critical_service_outage) | Outage of the critical service. |
| Event (sn_oper_res_event) | Event recorded for the application. |
| Failed control (sn_oper_res_failed_control) | Failed control. |
| GRC Profile (sn_grc_profile) | List of all GRC entities. |
| Importance impact tolerance assessment (sn_oper_res_importance_impact_tolerance_assessment) | Importance of the impact tolerance assessment. |
| Incident (sn_oper_res_incident) | Incident registered due to an event. |
| Issue (sn_oper_res_issue) | Issue logged due to an event. |
| M2M analysis participant (sn_oper_res_m2m_analysis_participant) | Association between analysis and participant. |
| M2M analysis scenario event (sn_oper_res_m2m_analysis_scenario_event) | Association between analysis and scenario event. |
| M2M scenario analysis service (sn_oper_res_scenario_analysis_service) | Association between scenario and analysis service. |
| M2M scenario event (sn_oper_res_m2m_scenario_event) | Association between scenario and event. |
| M2M service importance impact tolerance assessment (sn_oper_res_m2m_service_importance_impact_tolerance_assessment) | Association between service and importance of the impact tolerance assessment. |
| Operational Resilience profile (sn_oper_res_profile) | Operational Resilience entity. |
| Profile type (sn_grc_profile_type) | List of all GRC entity types. |
| Risk (sn_oper_res_risk) | Risk defined in the application. |
| Scenario (sn_oper_res_scenario) | Scenario defined in the application. |
| Scenario analysis (sn_oper_res_scenario analysis) | Scenario analysis defined in the application. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tables installed with Operational Resilience (continued)**

| Table name | Description |
|---|---|
| Service impact analysis (sn_oper_res_service_impact_analysis) | Service impact analysis defined in the application. |
| Service process pillar (sn_oper_res_service_process_pillar) | Service process pillar defined in the application. |
| Task (sn_oper_res_task) | Task defined in the application. |
| Vulnerability profile (sn_oper_res_vul_profile) | Vulnerability profile defined in the application. |
| Tables added in the Utah release | |
| M2M scenario event participant (sn_opres_res_m2m_scenario_event_participant) | Each participant can be associated to one or more scenario events. This table stores many-to-many relationships between the participant and scenario events. |
| M2M scenario event issue (sn_oper_res_m2m_scenario_event_issue) | Stores many-to-many relationships between the issues and scenario events. |
| Service related information (sn_oper_res_service_related_info) | Service related information defined in the application. |
| Service Summary (sn_oper_res_service_summary) | Service summary defined in the application. |
| Response tasks (sn_oper_res_resp_task) | Service tasks defined in the application. |
| Response tasks (sn_oper_res_response_task) | Response tasks that are defined in the application. |

## Domain separation and Operational Resilience

Domain separation is supported for Operational Resilience. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

## Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

For more information on support levels, see Application support for domain separation.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Overview

Operational Resilience supports domain separation. The tables are striped with the domain ID and domain path. Domain separation for Operational Resilience means that only a user in the application's domain or parent domain can access the data. All functionality for Operational Resilience works in a domain-separated environment as long as all of the following actions are performed by users within that domain:

- Create application
- Create/upload configuration data
- Perform scenario analysis
- Measure the importance and impact of your business service
- Self-attest your Operational Resilience status

### How domain separation works in Operational Resilience

Domain separation is supported only at the data level for Operational Resilience. Cross-level scheduled job data setup is not supported. Therefore, you must copy the scheduled job in each of your domain to respect the data level separation.

To set up domain separation for Operational Resilience:

1. Create your domain and then create Operational Resilience users in that domain.
2. Only a specified user (Operational Resilience admin in that domain) should populate configuration data in the application's domain.
3. Only users in the application's domain should upload or create data in the domain.

Follow these guidelines for successful domain separation:

- Create a separate user for each domain to perform upload, edit, or export of configuration data.
- Avoid uploading or creating configuration data for a given application in multiple domains.
- Only users in the application's domain should upload or create data in the domain.
- Policies and exporters must be either in the application's domain or in the global domain.

### Domain-separated tables in Operational Resilience

All Operational Resilience tables include a **Domain** column.

Related topics

Domain separation for service providers

## Policy and Compliance Management

The ServiceNow® Policy and Compliance Management product provides a centralized process for creating and managing policies, standards, and internal control procedures that are cross-mapped to external regulations and benchmarks. Additionally, the application provides structured workflows for the identification, assessment, and continuous monitoring of control activities.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| | | |
|---|---|---|
| **Explore**<br>  <br>Explore key features and benefits of Policy and Compliance Management | **Configure**<br>  <br>Set up checklist for the GRC: Policy and Compliance Management application | **Administer**<br>  <br>Components installed with Policy and Compliance Management |
| **Use**<br>  <br>Use the Compliance Workspace for compliance tasks | **Build**<br>  <br>Author and redline policy documents in Compliance Workspace | **Manage**<br>  <br>Mobile experience for GRC Policy and Compliance |
| **Integrate**<br>  <br>Use UCF Common Controls Hub to manage compliance frameworks | **Analytics and Reporting**<br>  <br>Analytics and reporting solutions for compliance records | |

### Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

### Activate Policy and Compliance Management

The Policy and Compliance Management (com.sn_compliance) plugin is available as a separate subscription and requires activation.

### Troubleshoot and get help

- Ask or answer questions in the GRC community
- Search the Known Error Portal for known error articles
- Learn how to build apps on the developer site.
- Contact Customer Service and Support

## Exploring Policy and Compliance Management

The ServiceNow® Policy and Compliance Management product provides a centralized process for creating and managing policies, standards, and internal control procedures that are cross-mapped to external regulations and benchmarks. Additionally, the application

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

provides structured workflows for the identification, assessment, and continuous monitoring of control activities.

## Policy and Compliance Management overview

A comprehensive integrated risk management (IRM) program is defined by the requirements established by an organization's policies. For instance, controls may mitigate risk, but they are primarily implemented to enforce policies. Therefore, the normalization and consolidation of policies is an integral step in an organization's strategy in order to manage risk and meet compliance requirements across an ever-growing regulatory landscape.

The scope of Policy and Compliance Management includes:

- Process to create policies and controls.
- Control risk exposure by continuously monitoring risks and control or configuration changes.
- Reduce manual burden and cost through automation.

The process objectives of Policy and Compliance Management are:

- Create a centralized platform for creating policies, control objectives, and controls and map them to regulations and industry guidelines.
- Manage the lifecycle of policies with a consistent process.
- Communicate policies across the organization using a tool.
- Assess the state of compliance.
- Provide a systematic and consistent approach to managing the lifecycle of controls.

Policy and Compliance Management centralizes the following activities:

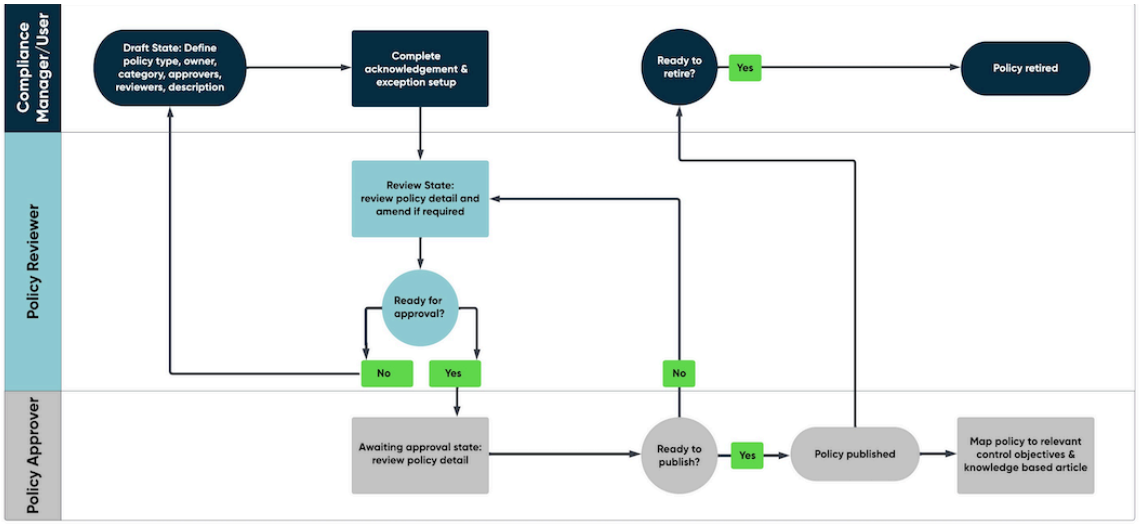
- Establish controls and control owners
- Define control tests and expected results
- Establish test and control frequencies
- Identify risks: impact and likelihood
- Prepare attestations
- Map authoritative sources to policies, procedures, controls, and risks

## Policy lifecycle

Policies ensure compliance and reduce exposure to risks. Publishing a policy is automatically incorporated in the approval process. Policies have a type, such as a policy, procedure, standards, plan, checklist, framework, or template.

As a compliance admin or compliance manager you can create a policy. When you create a policy, it is in a state of Draft as the policy record is opened, and all the required information about the policy are defined and captured in the record. The required information that you capture are the attributes that drive the process flow of the policy.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

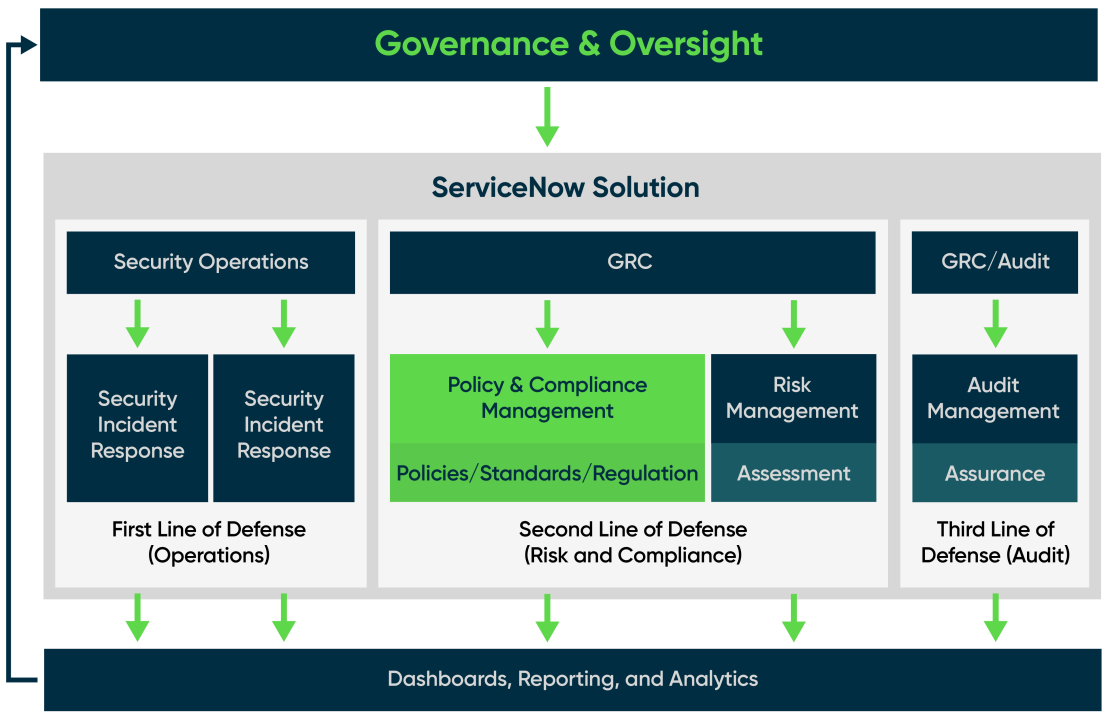



## Policy and Compliance Management users

Policy and Compliance activities involve all levels of management. A key function of good governance involves the establishment of a strong organization structure.

- Board of directors
- IT steering committee
- Audit committee
- All levels of management

## Policy and Compliance Management and the Now Platform

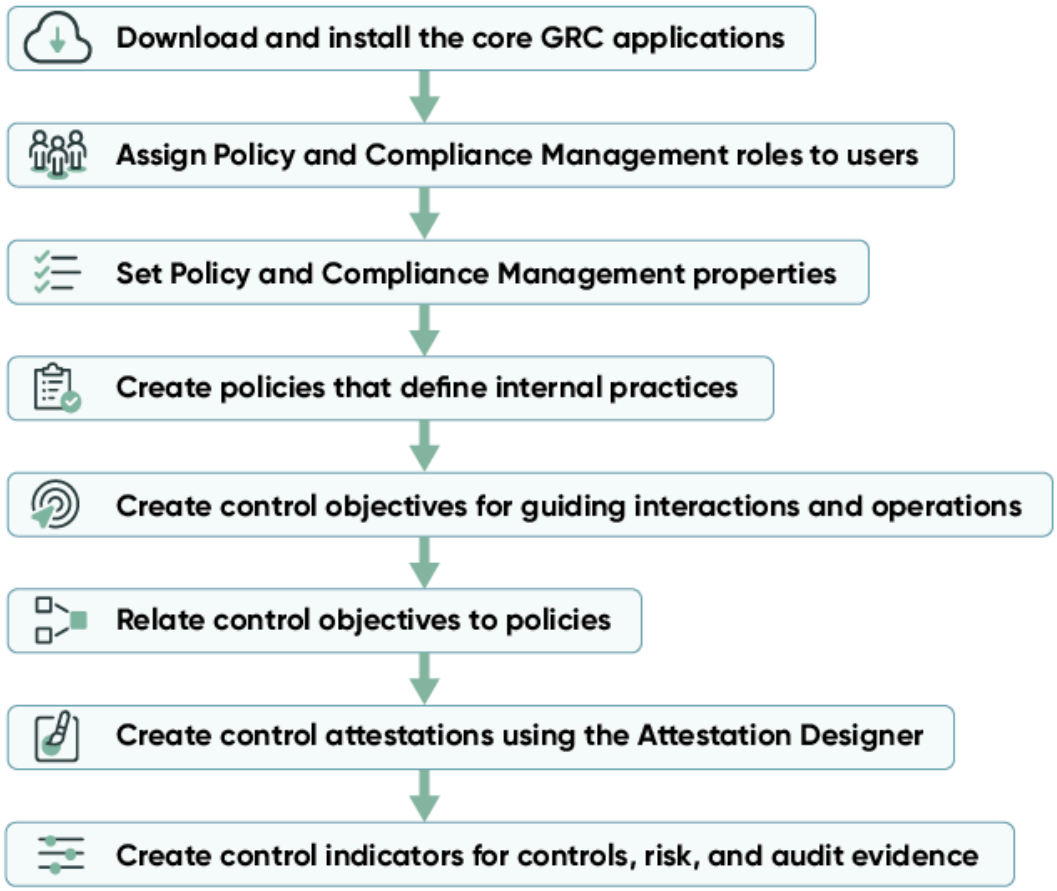



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Implementing Policy and Compliance Management

Use the steps in the GRC: Policy and Compliance Management application checklist to download the Policy and Compliance Management from the ServiceNow Store, and get it ready for operation. Mandatory and optional setup steps, as well as an implementation checklist are provided to simplify the setup.

The flow of mandatory steps in the checklist are illustrated here.




When you have completed the mandatory steps outlined above, other optional setup procedures are available.

## Setup checklist for the GRC: Policy and Compliance Management application

This checklist includes the setup tasks that you are required to complete in your Now Platform® instance. When you have completed these tasks, the base system is ready for operation. Optional setup procedures are also included to enhance GRC: Policy and Compliance Management functionality.

### Before you begin

Role required: sn_compliance.admin, sn_compliance.manager
Consider creating and printing a PDF of this checklist topic. You can then check off tasks as you complete them.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

To generate a PDF, click the **Save As PDF** icon (  ) at the top of the topic and click **Selected topic**.

### GRC: Policy and Compliance Management application checklist

| Item | Description |
|---|---|
| ☐ | As a user with the Compliance Administrator or Compliance Manager role, verify that you have the GRC core applications installed on a Now Platform instance.<br><br>**Note:** The GRC core applications and the Now Platform instance should be from the same family release.<br><br>**a.** To verify the GRC: GRC Profile Dependencies core application is installed on your instance, navigate to **Plugins** and search for GRC Profile.<br>**b.** If the GRC Profile core application is not already installed, click **Install** to install it.<br>**c.** After the GRC Profile application is installed, install the Policy and Compliance Management core application.<br><br>If Policy and Compliance Management is not visible in your instance, all of the GRC core applications are available from the ServiceNow Store. For more information about getting entitlement, downloading, and installing the GRC core applications, see GRC and the ServiceNow Store. |
| ☐ | As a user with the Compliance Administrator role, in your Now Platform instance, verify that you have assigned users with the required Now Platform roles.<br><br>For detailed instructions and a list of Policy and Compliance Management roles, see Assign Policy and Compliance Management roles to your users. |
| ☐ | As a user with the Compliance Administrator role, set Policy and Compliance Management properties to control various behaviors in the system. For example, you can define states for which a control is active or inactive.<br><br>For detailed instructions, see Set Policy and Compliance Management properties. |
| ☐ | As a user with the Compliance Administrator or Compliance Manager role, create policies. A policy is a document that defines an internal practice that processes must follow. Policies are defined as policies, procedures, standards, plans, checklists, frameworks, and templates.<br><br>For detailed instructions, see Create a policy. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Item | Description |
|---|---|
| ☐ | As a user with the Compliance Administrator or Compliance Manager role, create control objectives. A control objective is an objective, direction, or standard that acts as guidance for company interactions and operations. They can be categorized, classified, and related to policies.<br><br>For detailed instructions, see Create a control objective. |
| ☐ | As a user with the Compliance Administrator or Compliance Manager role, relate control objectives to policies. You can associate control objectives to a policy individually when the policy is in the Review or Draft state.<br><br>For detailed instructions, see Relate a control objective to a policy. |
| ☐ | As a user with the Compliance Administrator, Compliance Manager, or Attestation Creator role, create an attestation. The Attestation Designer allows you to create and edit metric types, as well as define different metric types for different controls.<br><br>For detailed instructions, see Create a control attestation using the Attestation Designer. |
| ☐ | As a user with the Compliance Administrator or Compliance Manager role, create control indicators. Indicator data for controls, risk, and audit evidence are measured differently depending on the GRC application.<br><br>For detailed instructions, see Create a control indicator. |

Congratulations! You have successfully set up the GRC: Policy and Compliance Management base system. Depending on the needs of your organization, optional setup procedures are available. For example, if you integrate with Network Frontiers Unified Compliance Framework (UCF), procedures for managing the integration are here. Or if you want to set up the mobile experience for GRC: Policy and Compliance Management, those procedures are also here.

For detailed instructions for optional features, see Policy and Compliance Management enhancement steps.

## Download GRC: Policy and Compliance Management

Before you run GRC: Policy and Compliance Management (com.sn_compliance) in your instance, you must download it from the ServiceNow Store.

### Before you begin

Role required: admin

### Procedure

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** Starting with Version 10.1, you can leverage new policy exception capabilities in Policy and Compliance Management from within Version 10.3 of the Vulnerability Response application. To use this feature, you must upgrade Policy and Compliance Management before upgrading Vulnerability Response. For more information, see

Related topics

List of plugins

### Quick start tests for Policy and Compliance Management

Validate that GRC: Policy and Compliance Management still works after you make any configuration change, such as apply an upgrade or develop an application. Copy and customize these quick start tests to pass when using your instance-specific data.

GRC: Policy and Compliance Management quick start tests require activating the Policy and Compliance Management plugin (com.sn_compliance) and loading the demo data.

#### GRC: Policy and Compliance Management Quick Start Tests test suite

| Test | Description | Release version |
|---|---|---|
| GRC: Create Controls | Validates control creation. | Madrid |
| GRC: Create Policy Exception and Flow | Create a policy exception and navigate through its states. | Paris |
| GRC: Policy Lifecycle | Create a policy and navigate through its states. | Paris |

Related topics

Quick start tests

## Perform Policy and Compliance Management administration

Prior to performing application-specific setup, you need to prepare the system. This involves assigning user roles and setting properties.

### Assign Policy and Compliance Management roles to your users

Before you can successfully implement or use the Policy and Compliance Management application, you must assign roles to your users.

#### Before you begin

Role required: admin

#### Procedure

1. Navigate to **All** > **User Administration** > **Users**.
2. Click the name of a user.
3. Click the **Roles** tab.
4. Click **Edit**.
5. Move the roles you want to assign to the user from the Collection side to the Roles List, then click **Save**.
6. Repeat these steps for each of your users.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role title [name] | Description |
| --- | --- |
| Compliance Reader<br><br>[sn_compliance.reader] | The Compliance Reader has read-only access to all modules of the Policy and Compliance Management application. This role is typically assigned to users who need to see what policies and controls are within the organization. Users with the reader role are also often responsible for reporting and monitoring activities.<br><br>The Compliance Reader role contains: sn_grc.reader. |
| Compliance User<br><br>[sn_compliance.user] | The Compliance User, often referred to as the Compliance Analyst, has permissions enough to fulfill virtually any policy- or control-related task.<br><br>Users assigned this role are often responsible for:<br>◦ Creating new policies<br>◦ Requesting policy exceptions<br>◦ Responding to acknowledgement requests<br>◦ Creating controls objectives and relating them to policies<br>◦ Testing and monitoring control effectiveness<br>◦ Attesting controls<br>◦ Remediating issues<br>◦ Assisting with risk assessments and audit tasks<br><br>The Compliance User role contains:<br>◦ sn_grc.reader<br>◦ sn_grc.user<br>◦ sn_compliance.reader<br><br>**Note:** Users with the Compliance User role can be assigned controls, and have read-only access to the Risk Management application and modules. |
| Compliance Manager<br><br>[sn_compliance.manager] | The Compliance Manager is responsible for managing the day-to-day compliance process. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role title [name] | Description |
| --- | --- |
| | Users assigned this role are often responsible for:<br>◦ Reviewing specific regulatory requirements and trends<br>◦ Determining which regulations require a policy<br>◦ Approving policies and policy exceptions<br>◦ Setting up a policy acknowledgement campaign<br>◦ Scoping controls using entity types and entities<br>◦ Creating and assigning attestations<br>◦ Continuously monitoring control effectiveness<br>◦ Compiling and sharing reports highlighting data, such as non-compliant controls<br>The Compliance Manager role contains:<br>◦ sn_grc.reader<br>◦ sn_grc.user<br>◦ sn_grc.manager<br>◦ sn_compliance.reader<br>◦ sn_compliance.user |
| Compliance Administrator<br>[sn_compliance.admin] | The Compliance Administrator administers the Policy and Compliance Management application.<br>Users assigned this role are often responsible for:<br>◦ Monitoring platform dependencies with other applications and modules<br>◦ Controlling all compliance data<br>The Compliance Administrator role contains:<br>◦ sn_grc.reader<br>◦ sn_grc.user<br>◦ sn_grc.manager<br>◦ sn_grc.admin<br>◦ sn_compliance.reader<br>◦ sn_compliance.user<br>◦ sn_compliance.manager |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role title [name] | Description |
|---|---|
| Compliance Developer<br><br>[sn_compliance.developer] | The Compliance Developer is responsible for maintaining various aspects of the platform, such as creating workflows, reports, dashboards, additional modules, and other platform-specific content that can enrich the application.<br><br>The Compliance Developer role contains:<br>◦ sn_grc.reader<br>◦ sn_grc.user<br>◦ sn_grc.manager<br>◦ sn_grc.admin<br>◦ sn_grc.developer<br>◦ sn_compliance.reader<br>◦ sn_compliance.user<br>◦ sn_compliance.manager<br>◦ sn_compliance.admin |
| Attestation Creator<br><br>sn_compliance.attestation_creator | The Attestation Creator is responsible for creating and maintaining attestations. Attestations are one of the platform components used to attest controls and it is essential for keeping them lean, precise, and up-to-date. |

### What to do next
Return to the Policy and Compliance Management setup checklist.

### Set Policy and Compliance Management properties

Set properties to control various aspects and behaviors in the software.

### Before you begin
Role required: admin

### Procedure

Navigate to **All** > **Policy and Compliance** > **Administration** > **Properties**.

| Name | Description |
|---|---|
| States for which the control is active (the first state is the default active state)<br><br>sn_compliance.active_states<br><br>**Note:** Controls in active states only, as mentioned in this property, are considered during compliance score calculation. | Compliance administrators can change this setting.<br>• **Type**: string<br>• **Default value**: draft, assess, review, monitor |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Name | Description |
| --- | --- |
| | • **Location**: **Policy and Compliance** > **Administration** > **Properties** |
| States for which control is inactive (the first state is the default inactive)<br><br>sn_compliance.closed_states<br><br>**Note:** Controls in inactive states, as mentioned in this property, are not considered during compliance score calculation. | Compliance administrators can change this setting.<br>• **Type**: string<br>• **Default value**: retired<br>• **Location**: **Policy and Compliance** > **Administration** > **Properties** |
| Name of the assessment metric type that is used for attestations<br><br>sn_compliance.default_attestation | System administrators can change this setting.<br>• **Type**: string<br>• **Default value**: GRC Attestation<br>• **Location**: **Policy and Compliance** > **Administration** > **Properties** |
| This is a platform-level system property that is used to run client scripts in strict mode with direct DOM disabled. When this property is set to true, you cannot use jquery or change the DOM directly.<br><br>sn_compliance.glide.script.block.client.globals | • **Type**: true or false<br>• **Default value**: false<br>• **Location**: **Policy and Compliance** > **Administration** > **Properties** |
| Name of the knowledge base used to publish Policy articles<br><br>sn_compliance.knowledge_base | Compliance administrators can change this setting. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

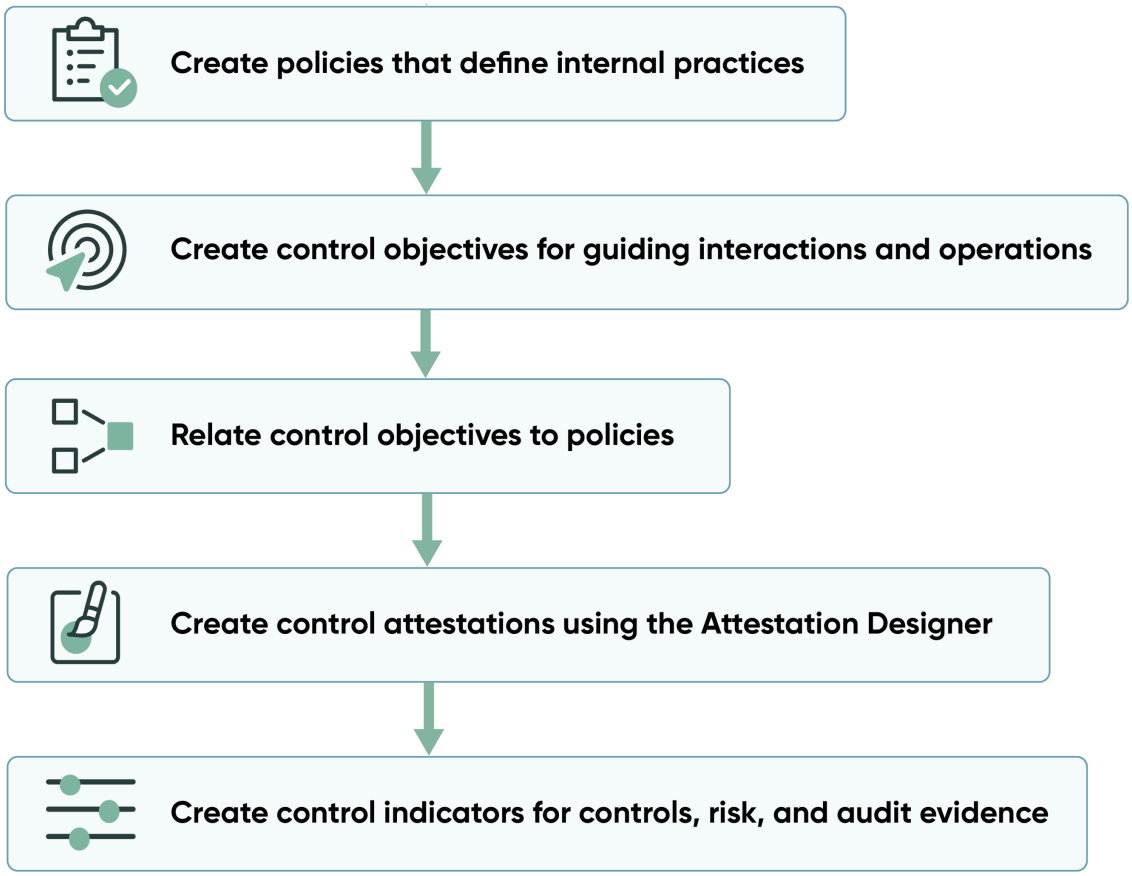
| Name | Description |
| --- | --- |
| | • **Type**: string<br>• **Default value**: Governance, Risk, and Compliance<br>• **Location**: **Policy and Compliance** > **Administration** > **Properties** |

**What to do next**
Return to the Policy and Compliance Management setup checklist.

## Policy and Compliance Management mandatory setup

After you have assigned roles to your users and set Policy and Compliance Management properties, proceed with the mandatory setup steps.

The flow of mandatory steps in the checklist are illustrated here.




When you have completed the mandatory steps outlined above, other optional setup procedures are available.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Create a policy

A policy defines an internal practice that processes must follow. Policies are defined as policies, procedures, standards, plans, checklists, frameworks, and templates.

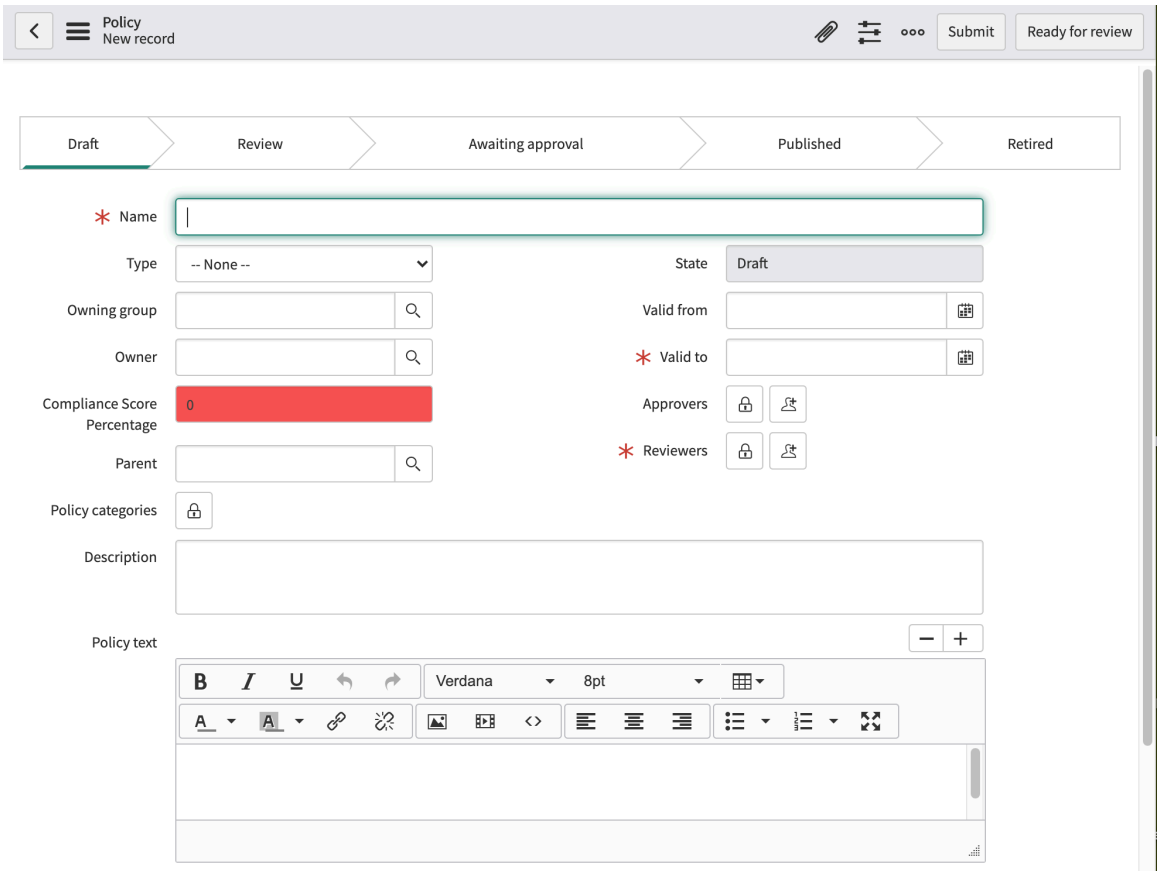
### Before you begin

Role required: sn_compliance.admin or sn_compliance.manager

Users with Compliance user (sn_compliance.user) role can also create policies.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Policies**.
2. Click **New**.




3. On the form, fill in the fields.

#### Policy

| Field | Description |
|---|---|
| Name | The name of the policy. |
| Type | List of options:<br>◦ Policy<br>◦ Procedure<br>◦ Standard |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ Plan<br>◦ Checklist<br>◦ Framework<br>◦ Template |
| Owning Group | Group that owns the policy. |
| Owner | User that owns the policy. |
| Compliance Score Percentage | The compliance score percentage assigned to this policy. |
| Parent | The policy containing this policy. If you create a control objective from within a policy, this field is automatically filled. |
| Policy categories | Click the lock icon and select one or more categories for filtering policies. For example, select Vulnerability Response to view policies associated with that application. |
| State | The state is a read-only field. Possible choices are:<br>◦ **Draft** In this state, all compliance users can modify the policy and control objectives. All compliance users can click **Request review** button. Enter a message in the Request review pop-up and click **Request** , which sets the state to Review.<br>◦ **Review** In this state, the owner, owning group, and reviewers can modify the policy and control objectives. The owner, owning group, and reviewers click **Request approval**, starting the workflow by sending approvals to the users in the Approvers list. The owner, owning group, and reviewers move the policy back to Draft, by clicking **Back to draft**, as well.<br>◦ **Awaiting approval** In this state, the policy and control objectives are read- only for all. Approvers can approve the policy by updating the approval state in the **Approvals** Related List on the policy form, or by viewing **My Approvals**. If the policy is approved, the policy goes to the **Published** state. Otherwise, it goes back to the **Review** state.<br>◦ **Published** In this state, the policy and control objectives are read-only for all. Admins can click **Retire** which sets the state of the policy to **Retired**<br>◦ **Retired** In this state, the policy is read-only for all. |
| Valid from | The date and time for which the policy becomes valid. |
| Valid to | The date and time for which the policy is no longer valid. |
| Approvers | The users you want to be included in the approval process. |
| Reviewers | Select the users you want to be included in the review process. |
| Description | A general description of the policy. |
| Policy text | A detailed description of the policy. |
| Knowledge Base | |
| Knowledge base | The knowledge base article related to this policy. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| KB article | The KB article number and link where the policy is published. |
| Article template | The article template to use for the publication of this policy. |
| Acknowledgement Setup | |
| Audience | Select the default audience responsible for acknowledging this policy. |
| Reference Material URL | Click the lock icon to add the URL for any needed reference materials, such as certification or training materials. |
| Allow users to decline policy | Select this check box to give users the option of declining policy acknowledgements. |
| Allow users to request exception | Select this check box to give users the option of requesting exceptions for policy acknowledgements. |
| Exception Setup | |
| Maximum exception duration (days) | Enter the maximum number of days for which a policy exception can be requested for a given policy. |

4. Continue with one of the following options.
   - To save and submit the policy, click **Submit**.
   - To mark the policy ready for review, click **Request review** .

### What to do next

If you are implementing the Policy and Compliance Management software, return to the Policy and Compliance Management setup checklist and proceed to the next step.

## Create a control objective

A control objective is an objective, direction, or standard that acts as guidance for company interactions and operations. Control objectives can be categorized, classified, and related to policies.

### Before you begin

Role required: sn_compliance.admin, sn_compliance.manager, sn_compliance.user

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Control Objectives**.
2. Click **New**.
3. On the form, fill in the fields.

#### Control Objectives form

| Field | Description |
|---|---|
| Name | Name of the control objective. |
| Source | Source of the control objective. For example, if the control objective is from a third-party provider, indicate which one. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Source ID | Unique identification number used by the source to catalog this control objective. |
| Reference | Unique numerical identifier. |
| Parent | Control objective that is not a child of the current control objective. This is to avoid cyclic parent – child relationship. |
| Compliance Score Percentage | Compliance score percentage calculated for this control objective and it's color code:<br>◦ 80 and higher in green<br>◦ 80 to 50 in yellow<br>◦ below 50 in red |
| Active | Option that indicates whether a control objective is active. |
| Creates controls automatically | Option that indicates that controls are automatically created from the control objective.<br>**Note:** Select this option if the control objective can also serve as the control. |
| Category | List of options:<br>◦ Acquisition or sale of facilities, technology, and services<br>◦ Audits and risk management<br>◦ Compliance and Governance Manual of Style<br>◦ Human Resources management<br>◦ Leadership and high-level objectives<br>◦ Monitoring and measurement<br>◦ Operational management<br>◦ Physical and environmental protection<br>◦ Privacy protection for information and data<br>◦ Records management<br>◦ System hardening through configuration management<br>◦ Systems continuity<br>◦ Systems design, build, and implementation<br>◦ Technical security<br>◦ Third Party and supply chain oversight<br>◦ Root<br>◦ Deprecated |
| Classification | List of options:<br>◦ Preventive<br>◦ Corrective<br>◦ Detective |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Type | List of options:<br>◦ Acquisition/Sale of Assets or Services<br>◦ Actionable Reports or Measurements<br>◦ Audits and Risk Management<br>◦ Behavior<br>◦ Business Processes<br>◦ Communicate<br>◦ Configuration<br>◦ Data and Information Management<br>◦ Duplicate<br>◦ Establish Roles<br>◦ Establish/Maintain Documentation<br>◦ Human Resources Management<br>◦ Investigate<br>◦ IT Impact Zone<br>◦ Log Management<br>◦ Maintenance<br>◦ Monitor and Evaluate Occurrences<br>◦ Physical and Environmental Protection<br>◦ Process or Activity<br>◦ Records Management<br>◦ Systems Continuity<br>◦ Systems Design, Build, and Implementation<br>◦ Technical Security<br>◦ Testing<br>◦ Training |
| Attestation | List of options.<br>◦ **GRC Attestation** is chosen by default<br>◦ **Note:** If the user changes the control attestation, the related control objective attestation type is changed also. |
| Issue group rule | Group rule assigned to this control objective. |
| Description | Description of the control objective. |

4. Click **Submit**.
   The control objective is created and all related lists are visible.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- A control is created for every control objective when a policy is associated with an entity.
- The control attributes default to the same attributes as the related control objective.

### What to do next

If you are implementing the Policy and Compliance Management software, return to the Policy and Compliance Management setup checklist and proceed to the next step.

## Relate a control objective to a policy

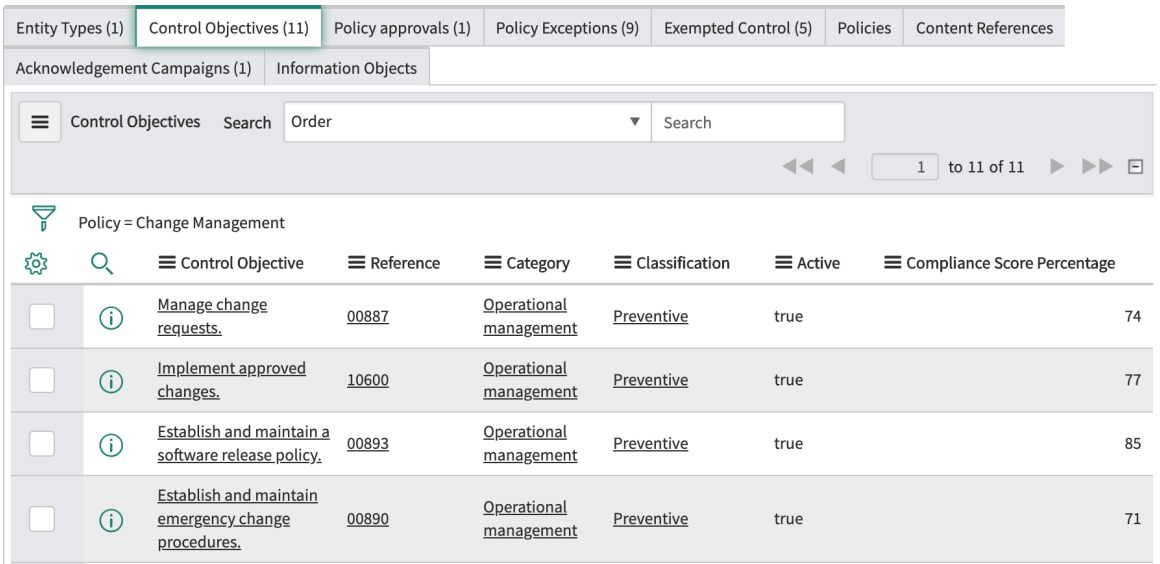
Associate the control objective to a policy individually when the policy is in the review or draft state by clicking the edit button in the Control Objective related list.

### Before you begin

Role required: sn_compliance.admin, sn_compliance.manager, sn_compliance.user

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Policies**.
2. Open the policy record.
3. Click **Edit** in the **Control Objectives** related list.
   The slushbucket contains active control objectives with no associated policy selected.
4. Select the control objectives.
5. Click **Save**.
   Those control objective are listed in the **Control Objective** related list.




### What to do next

If you are implementing the Policy and Compliance Management software, return to the Policy and Compliance Management setup checklist and proceed to the next step.

## Create a control attestation using the Attestation Designer

Use the Attestation Designer to create and edit metric types. Use different metric types for different controls. Select multiple respondents for an attestation, as well as change scoring parameters.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin

Role required: sn_compliance.attest_creator, sn_compliance.manager, sn_compliance.administrator

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Attestation Types**.
2. Click **Attestation Designer**.
   The designer contains the following elements:

| Element | Description |
|---|---|
| Controls | Supported question data types are available in the Controls palette. Drag a control onto the designer canvas to create a question of that type. |
| Questions | A library of questions for various categories, so you do not have to build each questionnaire from scratch. |
| Categories | New assessment opens in the **Design** view. The questionnaire **Name** field appears above the first category in the canvas. A blank question field appears in the category container. |

3. Enter a name in the **Name** field.
4. Drag a control onto the designer canvas to create a question of that type.

#### Question controls

| Data type | Description | Scored |
|---|---|---|
| Attachment | Question with a Manage Attachments icon that allows users to attach one or more files. | N |
| Boolean | Question with a check box or a **Yes/No** list for user responses. | Y |
| Choice | List of predefined options. For more information, see the definition for **Choices**. | Y |
| Date | Date field. | N |
| Date/Time | Date and time field. | N |
| Number | Number field with predefined minimum and maximum values. The default is 1–10. | N |
| Percentage | Percentage field with a prescribed range. | N |
| Scale | Predefined Likert scale. Answer options appear as radio buttons. | Y |
| Numeric Scale | Selectable number scale. The default is 1–5. Answer options appear as radio buttons. | Y |
| String | Single or multi-line text field. | N |
| Template | Choice list of templates that provide a predefined scale of options. | Y |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Data type | Description | Scored |
|---|---|---|
| | **Note:** It is important to assign a template to every attestation. This allows controls to be created automatically based on control objectives and entity types. | |
| Reference | Choice list of fields from a specified reference table. This data type does not support reference qualifiers. | N |

**Note:** Set the correct answer for the metric that you want to be scored. Scored metrics determine the compliance status of the controls.

5. Point to the menu icon in the upper right of the Attestation Designer to select one of the following options.

**Note:** The availability of each option depends on the status of the attestation that is opened in the designer.

| Option | Description |
|---|---|
| New Attestation | Opens a fresh canvas for a new attestation. |
| Load Attestation | Opens a list of existing attestations that you can select and edit. |

Unlike other types of assessments, control attestations do not appear in the **Self-Service** > **My assessments & surveys** module, because many control attestations could be generated at once. Instead, controls attestations are shown as a list in the **Policy and Compliance** > **Controls** > **My Attestations** module and **All Attestations** module.

### What to do next

If you are implementing the Policy and Compliance Management software, return to the Policy and Compliance Management setup checklist and proceed to the next step.

## Create a control indicator

Indicator data for controls, risk, and audit evidence are measured differently depending on the GRC application.

### Before you begin

Role required: sn_compliance_admin, sn_compliance_manager

### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Indicators** > **Indicators**.
   - **Risk** > **Indicators** > **Indicators**.
   - **Audit** > **Indicators** > **Indicators**.
2. Select **New**.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator form

| Field | Description |
|---|---|
| Category | Select **Compliance Indicator** for a control indicator and **Risk Indicator** for a risk indicator. |
| Name | Name of the indicator. |
| Applies to | Entity related to the **Item**. |
| Owning group | Group that owns the indicator. |
| Owner | Indicator owner. |
| Number | Unique identification number. |
| Active | Option that indicates whether the indicator is active. |
| Item | Related control or risk. |
| Template | Related indicator template. |
| Override Template | Option that indicates whether to override the indicator template associated to this indicator |
| Last result passed | Option that indicates whether the last result passed. |
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| Next run time | Next collection time for indicator results. |
| Method | |
| Type | Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script.<br>◦ Manual<br>◦ Basic |
| Short Description | If Type is **Manual**, this field is present. Brief description of the issue. |
| Instructions | If Type is **Manual**, this field is present. Instructions for the collection of indicator results. |
| Value Mandatory | If Type is **Manual**, this field is present. |
| Passed/Failed | If Type is **Basic**, this field is present. Indicator passes or fails. |
| PA Threshold | If Type is **PA Indicator**, this field is present. The associated PA Threshold. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Script | If Type is **Script**, this field is present. Script that obtains the desired system information. |
| Supporting Data | |
| **Note:** Starting with Version 10.1, the actual historical data for the supporting data records from the indicator results or indicator tasks is displayed. Earlier, only the real-time state of the records collected could be viewed. | |
| Table | Use supporting data to gather supporting evidence from other applications. |
| Supporting data fields | Supporting data fields based on the selected table. |

4. Select **Submit**.

**Note:** As a compliance manager or compliance admin, you can assign the indicator task to a user with Business User Lite role. If you assign a user with a Business User Lite role as an owner in the **Owner** field and **Execute** the indicator, an indicator task is created in the Open Tasks related list. This indicator task is assigned to the owner with the Business User Lite role.

As a user with the Business User Lite role, you can navigate to **Policy and Compliance** > **Indicators** > **My Indicator Tasks** to view the indicator tasks that are assigned to you. You can view the indicator by selecting the information icon next to the Indicator field. You can also update the **Result** field, **State** field, **Value** field, **Additional comments**, and **Work notes** in the Indicator Task form.

To accomplish similar tasks from the employee center, see GRC tasks in the employee center portal.

### What to do next

If you're implementing the Policy and Compliance Management software, then you've completed the required setup steps. Return to the Policy and Compliance Management setup checklist and proceed to the optional steps, as needed.

## Policy and Compliance Management enhancement steps

After you have set up the Policy and Compliance Management base system, you can perform the procedures listed in the following sections to enhance the functionality of the application.

Related topics

- Mobile experience for GRC Policy and Compliance
- Create a GRC article template
- Create or deactivate a citation
- Set notification properties
- Set up GRC Virtual Agent for requesting an exception to a policy or a control objective
- Allow policy exception requests from other applications

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Mobile experience for GRC Policy and Compliance

As a policy and compliance manager, use your Android or iOS mobile device to manage your work.

## Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

## Overview

As a user with the Now Platform® compliance manager (sn_compliance.manager) role, manage your work without being tied to the desktop. Receive timely notifications for current alerts, as well as risk and compliance status for your critical assets, vendors, and impacted essential business services all on your mobile device.

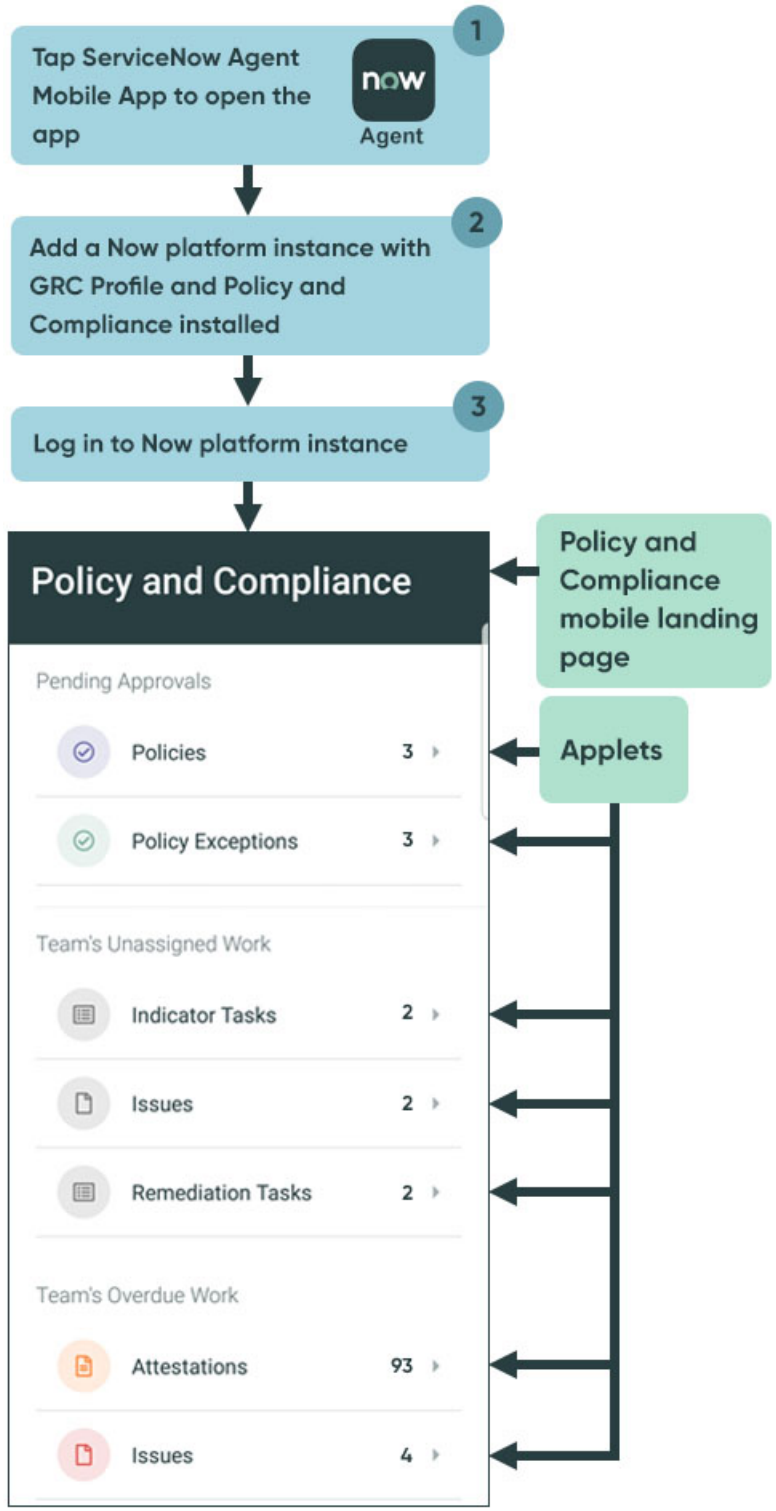
With the GRC Mobile application, you can perform the following Policy and Compliance Management activities without being tied to the desktop:

- Approve or reject pending Policies and Policy Exception requests that are assigned to you.
- Assign unassigned tasks and issues to your team with the Indicator Tasks, Issues, and Remediation Tasks applets.
- Manage and reassign your team's overdue tasks with the Attestations and overdue Issues applets.

The following figure illustrates how you log in to your Now Platform instance from your mobile device and the landing screen that is displayed after you log in.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### GRC Mobile application



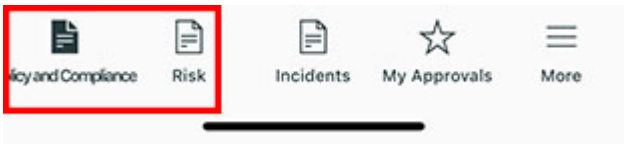

For step-by-step instructions about how to set up your Now Platform instance and install the GRC Mobile application, see Setup checklist for the GRC Mobile application. For instructions about how to log in, see Log in to the GRC Mobile application.

Applications

Applications are the ServiceNow® software components such as Policy and Compliance Management, Risk Management, and Audit Management that provide specific features and functionalities within your Now Platform instance. After you install these core applications and the GRC Mobile app on your Now

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Platform instance, these applications are displayed as icons on the bottom of your Android or iOS mobile device after you log in.




Folders

Each ServiceNow® mobile application contains folders that separate the applets by categories. In the preceding image, **Pending Approvals**, **Team's Unassigned Work**, and **Team's Overdue Work** are the folders of the Policy and Compliance Mobile app.

Applets

Applets are the different options within the application. In the preceding image, the icons under **Pending Approvals**, **Team's Unassigned Work**, and **Team's Overdue Work** are the available applets for the Policy and Compliance Mobile app.

### Setup checklist for the GRC Mobile application

The following checklist includes the set up tasks that you are required to complete in your Now Platform® instance and on your mobile device prior to using the GRC Mobile application. Complete these set up tasks prior to using the GRC Mobile application to view the Policy and Compliance Management application on your mobile device.

### Before you begin

As an option, print this checklist and use it to guide you through the set up tasks that are required for the GRC Mobile application.

Estimated time to complete this task: 15-20 minutes.

Roles required: admin, sn_compliance.manager

### Procedure

Verify that you complete each item on the list so that you can log in to the GRC Mobile application and add a Now Platform instance.

#### GRC Mobile application checklist

| Item | Description |
|---|---|
| ☐ | As a user with the admin role, verify that you have the GRC core applications installed on a Now Platform instance. This is the Now Platform instance that you view on your mobile device.<br><br>**Note:** The GRC core applications and the Now Platform instance should be from the same family release.<br><br>**a.** To verify the GRC: GRC Profile Dependencies core application is installed on your instance, navigate to **Plugins** and search for GRC Profile.<br><br>**b.** If the GRC Profile core application is not already installed, click **Install** to install it. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Item | Description |
| --- | --- |
| | **c.** After the GRC Profile application is installed, install either the Policy and Compliance Management core application, or the Risk Management core application, or both the Policy and Compliance Management and Risk Management applications. These are the two GRC applications that you can view with the GRC Mobile application.<br><br>If not visible in your instance, all of the GRC core applications are available from the ServiceNow Store.<br><br>For more information about getting entitlement, downloading, and installing the GRC core applications, see GRC and the ServiceNow Store.<br><br>When you install the GRC core applications, the dependency plugins for the GRC Mobile application, (com.glide.sg and com.glide.sg.agent_native_client) are also automatically installed.<br><br>To verify that these dependency plugins are installed and activated:<br><br>**a.** Navigate to **Plugins**.<br>**b.** Search for the plugin IDs (com.glide.sg and com.glide.sg.agent_native_client).<br>**c.** If they are not activated, activate these plugins. |
| ☐ | As a user with the admin role, verify that you have the GRC mobile app installed on the Now Platform instance that you want to view on your mobile device.<br><br>**Note:** The GRC mobile app and the Now Platform instance should be from the same family release.<br><br>For more information about getting entitlement, downloading, and installing the GRC Mobile application, see GRC and the ServiceNow Store. |
| ☐ | As a user with the admin role, in your Now Platform instance verify that you have assigned mobile users with the required Now Platform roles.<br><br>**a.** To view the roles that are assigned to a user, navigate to **Users and Groups** > **Users**.<br>**b.** Select the user name followed by the roles related list. All roles assigned to this user are displayed.<br>**c.** Verify a user is assigned, or assign a user with the IT Infrastructure Library role (itil). Users with the itil role can create, open, and update records. Only users with the itil role can have tasks assigned to them.<br>**d.** Verify a user is assigned, or assign a user with the compliance manager role (sn_compliance.manager). This role is automatically added when you assign the itil role.<br>**e.** Verify you have created any required assignment groups and assigned mobile users to these groups. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Item | Description |
|---|---|
| | **Note:** If you have multiple users for the mobile application, you alternatively can assign the sn_compliance.manager role to a group. Each user you add to the group inherits this role.<br><br>For more information on users and assigning roles to users and groups, see Create a user, Assign a role to a user, Assign a role to a group. |
| ☐ | As a mobile user with the sn_compliance.manager role, download and install the most current ServiceNow® Agent app on your mobile device.<br><br>The most current Agent app is available on the Apple iOS App Store and the Google Play Store.<br><br>  |
| ☐ | As a user with the sn_compliance.manager role, verify notifications are enabled on your mobile device and in your Now Platform instance.<br><br>Notifications inform you when critical pending approval requests are assigned to you or to your assignment group. To assist you with timely remediation, after you enable notifications, click on a notification in the GRC Mobile application and navigate directly to the record.<br><br>To enable notifications in your Now Platform instance so they are displayed on your mobile device, follow these steps.<br>**a.** Verify you have downloaded and installed the GRC Mobile application on your Now Platform instance.<br>**b.** In System Settings in your Now Platform instance, under Notifications, verify you have enabled the **ServiceNow Mobile Application**.<br><br>Now Platform notifications are also displayed on the messages screen on your mobile device. Verify that notifications are also enabled in the settings of your mobile device. |

You have successfully set up your mobile device and the Now Platform for the GRC Mobile application. The next step is to log in to your Now Platform instance with the ServiceNow Agent app on your mobile device.

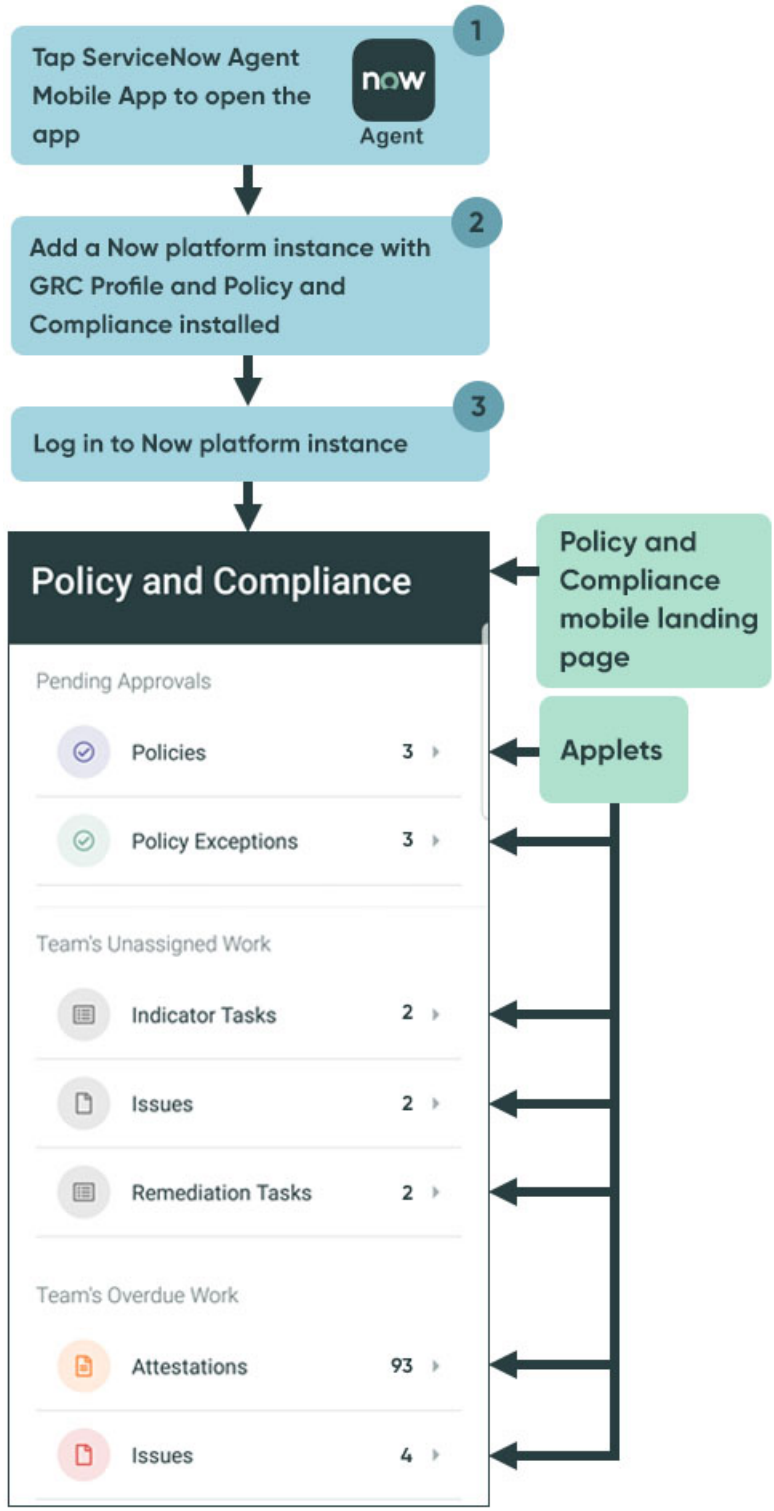
### Log in to the GRC Mobile application

Open the GRC Mobile application and add a Now Platform® instance with Policy and Compliance Management to your mobile device.

**Before you begin**
Verify that you have completed the setup steps described in Setup checklist for the GRC Mobile application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### GRC Mobile application




Role required: GRC Compliance manager (sn_compliance.manager)

**About this task**

Time to complete this task: 5-7 minutes.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. On your mobile device, tap the **ServiceNow Agent** app.

   If you are not already logged in to a Now Platform instance, the Instances screen is displayed.

2. If the Now Platform instance with the Policy and Compliance Management core application is not already added to your mobile device, follow these steps to add it.

   a. On the Instances screen that is displayed, tap the plus icon (  ).
   A screen is displayed that prompts you to enter and save an address of a Now Platform instance.

   b. Fill in the fields.

| Field name | Description |
|---|---|
| Enter the instance address or scan a QR code. | Choose one to continue:<br>▪ Before the `.service-now.com` in the field, enter the name of your Now Platform instance, for example, `grcmobile`.<br>▪ Enter an address. This address is the URL of your Now Platform instance that you want to view on your mobile device.<br>▪ Scan a QR code.<br>For more information about the mobile app, see "Log in to an instance with the mobile app" on the ServiceNow product documentation website. |
| (Optional) Enter nickname | Enter a nickname for this instance. If you have multiple instances added to the device, nicknames can help you quickly locate a Now Platform instance. |

   c. Tap **Save and Login**.

3. On the ServiceNow login screen that is displayed, enter the User name and Password for the Now Platform instance that you want to add and tap **Login**.
   The Policy and Compliance landing screen is displayed. You have successfully logged in to the GRC Mobile application.

4. After you log in, verify notifications are enabled in the GRC Mobile application.

   a. On the landing screen on the bottom, tap **More**.

   b. On the More screen, tap **Notification**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. On the Notifications screen, tap **Enable Notifications** if not enabled.
Notifications from the Now Platform are displayed on the Notifications screen in the GRC Mobile application.

5. After you log in to an instance on your mobile device, it is the default Now Platform instance on the device.
If you want to view another Now Platform instance on your device, you must log out of the default instance. To log out:

a. On the bottom of the screen, tap the **More**.
The More screen is displayed.

b. Tap **Settings**.

c. On the screen that is displayed, tap **Logout**.
The Instances screen is displayed with any Now Platform instances you have added to the mobile device.

d. Optional: Tap another instance to log in to it, or, alternatively, follow the preceding steps to add another instance.

**Trouble?**

If the instances screen for the GRC Mobile application is not displayed after you tap the **ServiceNow Agent** app on your device, verify that the **ServiceNow Agent** app is permitted as a trusted app on your device. To permit access as a trusted app, navigate to the settings and general device management on your device and tap the option (**Trust app**, etc.) to permit access.

If an error message is displayed after you enter your credentials in the log in screen, verify that your User name and password for the Now Platform instance is correct.

If you have problems viewing the landing screen, verify your network connection.

If you cannot view the Instances screen after you tap the **ServiceNow Agent** app, try uninstalling it from your device. Verify you have the most current version of the app from the Apple iOS App Store or the Google Play Store and try reinstalling it.

## What to do next

Select one of the following topics for more information about each applet.

### Process pending Policy and Compliance Management approval requests with the GRC Mobile application

Approve or reject pending policy approval requests that are submitted to you.

## Before you begin

Role required: Compliance manager (sn_compliance.manager)

## About this task

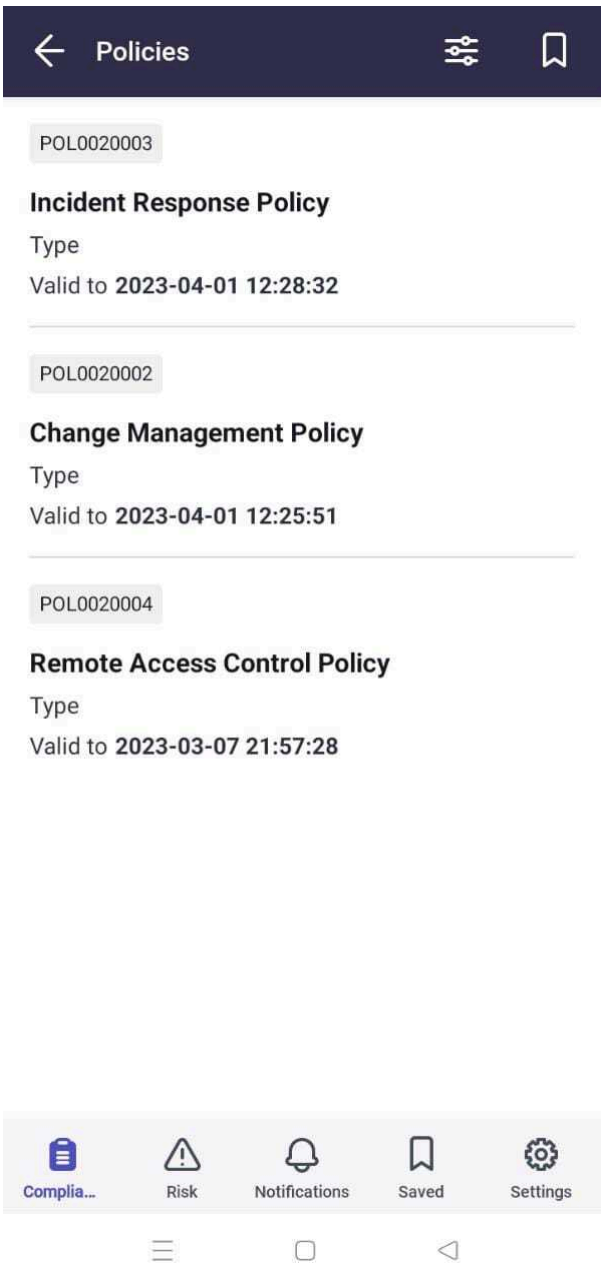
Approve or reject a pending Policy and Compliance Management request from the list of records. Alternatively, view the details of the record or add a work note prior to processing the request. Time to complete this task: 5-10 minutes.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

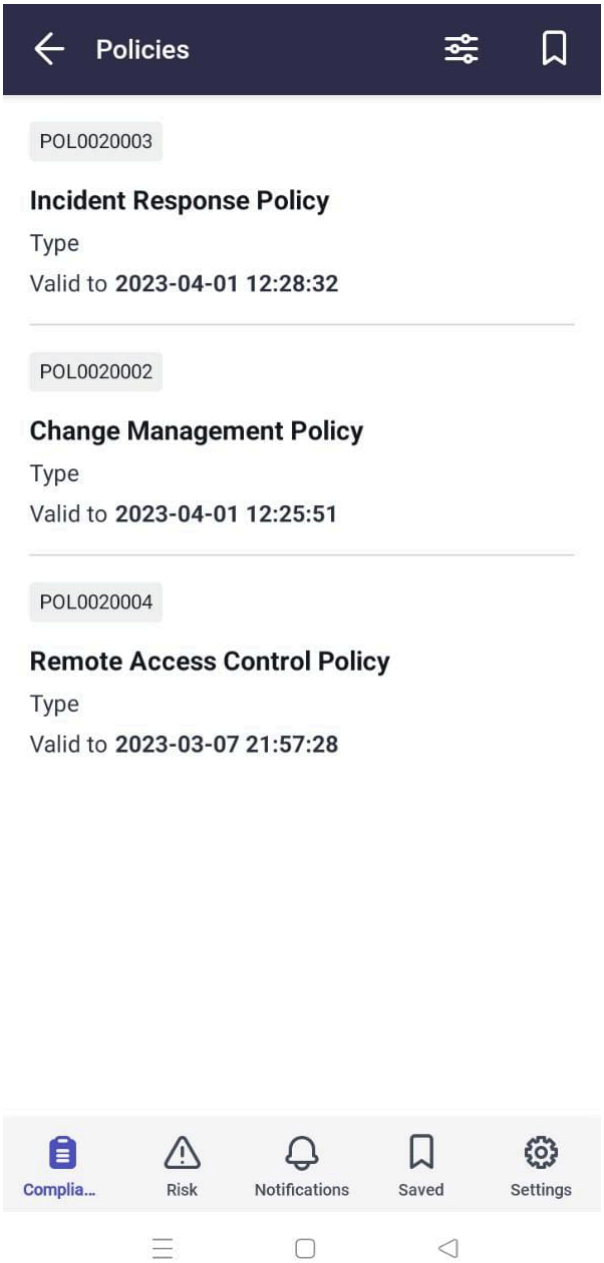
1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Policy and Compliance landing screen displayed, tap **Policies**.

   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.




   The Policies screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

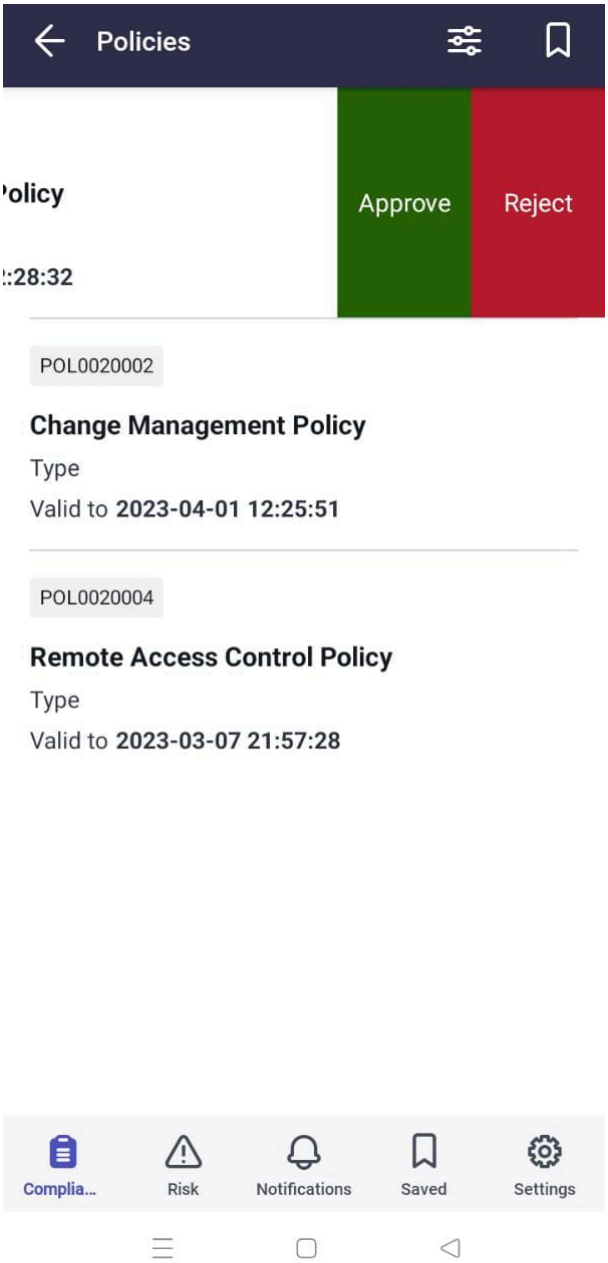



3. Optional: If you want to reduce the number of records that are displayed on the screen, see Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

4. With the Policies screen displayed with a list of records, swipe left on a record to open the menu.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



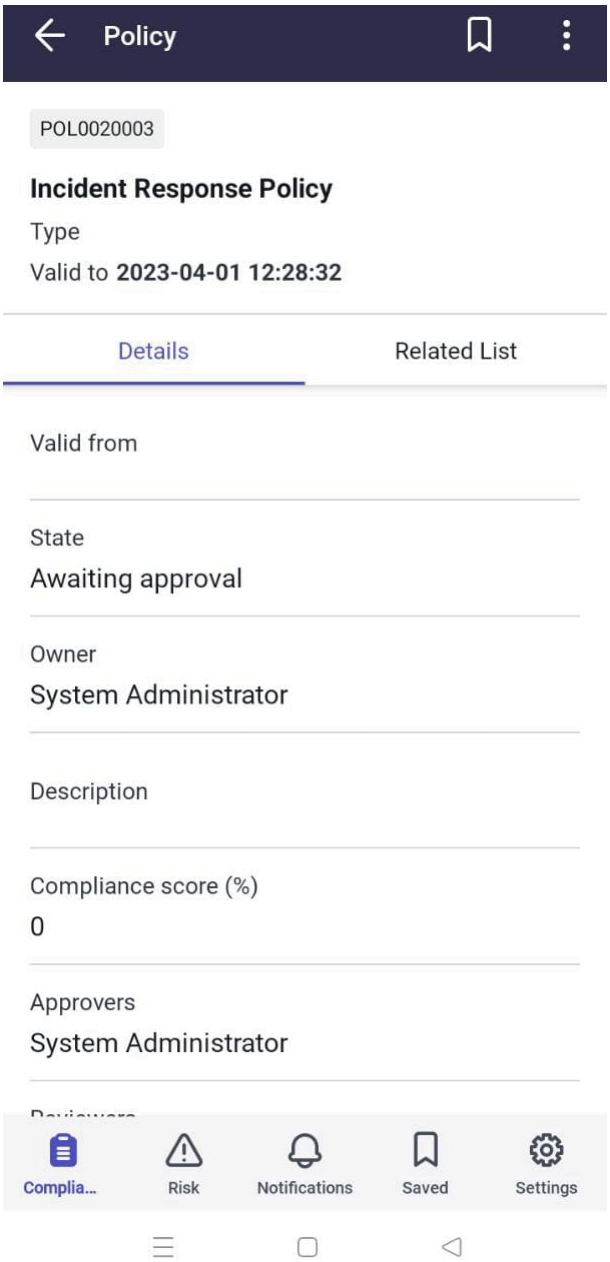

5. On the menu that is displayed, choose one to process the request.

| Option | Description |
|---|---|
| Approve. | In the Comments field, enter comments. Comments are optional for approvals. Tap the Send icon ( ) or **Submit** to save and submit your changes. |
| Reject. | In the Comments field, enter comments. Comments are required for rejections. Tap the Send icon ( ) or **Submit** to save and submit your changes. |

6. Alternatively, with the Policies screen displayed, tap a record on the list to open it and view more details.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

With the fields on the policy records displayed as shown in the following figure, choose one in the table to continue.




| Option | Description |
|---|---|
| Details tab | Choose one to continue.<br>◦ View the fields for details about the Policy.<br>◦ At the top right of the screen, tap the menu icon ( ) to approve or reject the policy approval request. Follow the steps described in the preceding table. |
| Related List tab | View the related lists. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | **a.** Tap **Control Objectives** to view the items on the Control Objectives related list.<br>**b.** On the list that is displayed, tap an item to open the record and view more details. If there are multiple records, use the filter to Filter records with the GRC Mobile application.<br>**c.** After you review the details, navigate back to the Policy screen and tap the menu icon (  ) to approve or reject the policy approval request. Follow the steps described in the preceding table. |
| Screen icons at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br>◦ Tap the Policy and Compliance icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br>◦ Tap **More**:<br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **Settings** followed by **Logout** to log out of the current instance. |

### Process pending approvals for Policy exceptions with the GRC Mobile application

Approve or reject pending policy exceptions and policy exception extension requests that are assigned to you.

#### Before you begin

Role required: Compliance manager (sn_compliance.manager)

#### About this task

With this applet, you can perform the following tasks on a list of policy exception records:

- Edit
- Request more information
- Approve, or reject pending policy exceptions or extension requests
- View the details of the record or add a work note prior to processing the request

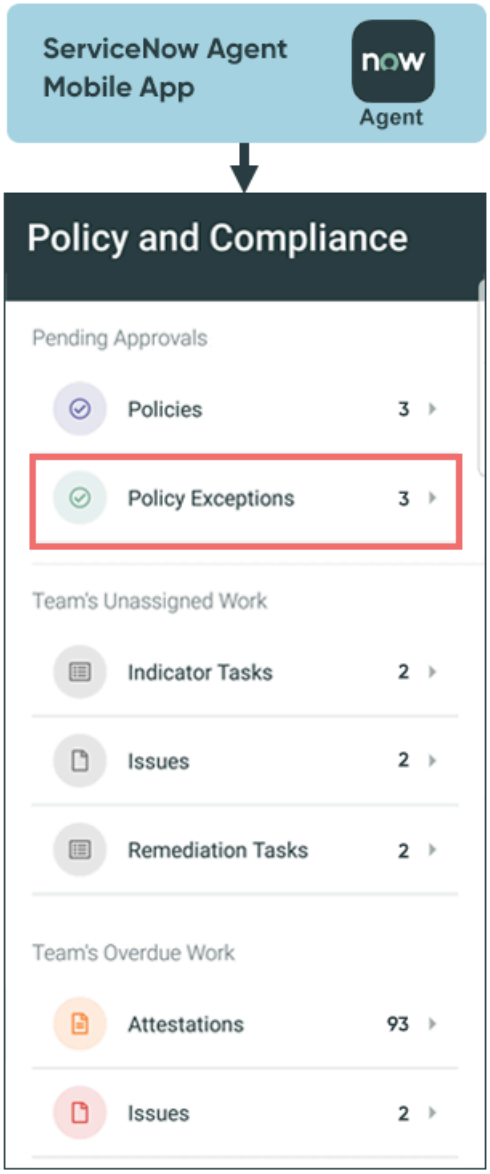
Time to complete this task: 5-10 minutes.

#### Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Policy and Compliance landing screen displayed, tap **Policy Exceptions**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.




The Policy Exceptions screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. Optional: If you want to reduce the number of records that are displayed on the screen, see Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To edit, approve or reject, or request more information about a policy exception directly from the list of records displayed on the screen, swipe left on a record to open the menu.




5. On the menu that is displayed, choose one from the following table to continue.

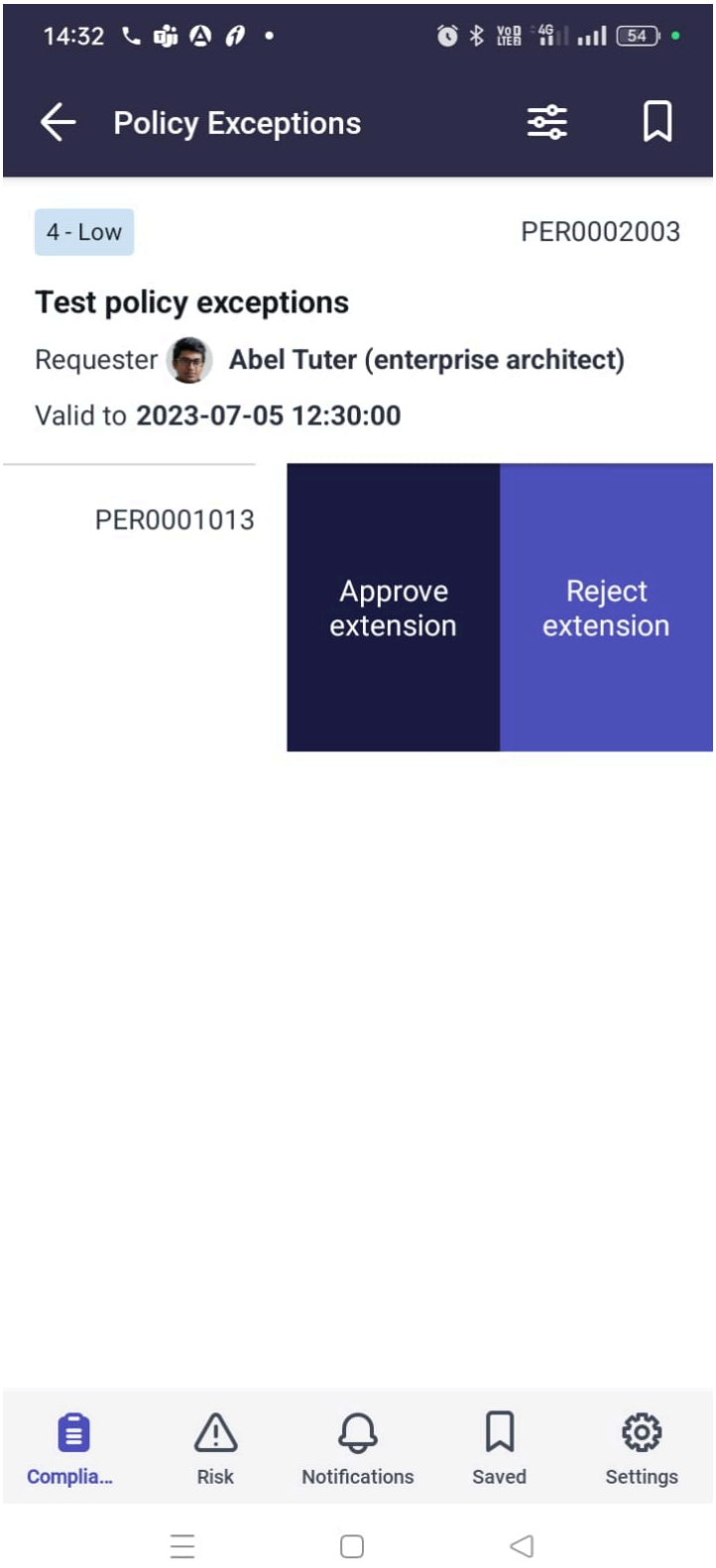
| Option | Description |
| --- | --- |
| Tap the menu icon (⋯) | From the fields that are displayed, choose one to continue.<br>◦ Tap **Request more information**.<br>In the Additional comments field, enter a comment to the user who requested the policy exception request. Your request is sent to the originator of the exception request and the extension number is included with your comment. Tap the send icon (➤) or **Submit** to submit your request.<br>After your request is sent, the option to request more information is no longer available from the menu until the requester provides the information and requests approval once again. If available, tap the **Activity Stream** tab on the policy exception record and refer to the work notes for the audit trail.<br>◦ Tap **Edit** and tap a field to edit the Valid from, Valid to, and Approver fields.<br>**Note:** Only users from your approval group are available for the Approver field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | Tap the Send icon ( ) or **Submit** to save and submit your changes.<br>◦ Cancel the operation and return to the exception record list. |
| Approve | In the Additional comments field, enter comments. Comments are optional for approvals. Tap the calendar icon to edit the Valid to date. Tap **OK** followed by the Send icon ( ) or **Submit** to save and submit your changes. |
| Reject | In the Additional comments field, enter comments. Comments are required for rejections. Tap the Send icon ( ) or **Submit** to save and submit your changes. |

6. To approve or reject a policy exception extension request directly from the list of records displayed on the Policy Exceptions screen after you have requested more information, swipe left on a record to open the menu.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**7.** On the menu for policy extension that is displayed, choose one to continue.

| Option | Description |
| --- | --- |
| Approve the extension | In the Additional comments field, enter comments. Comments are optional for approvals. |

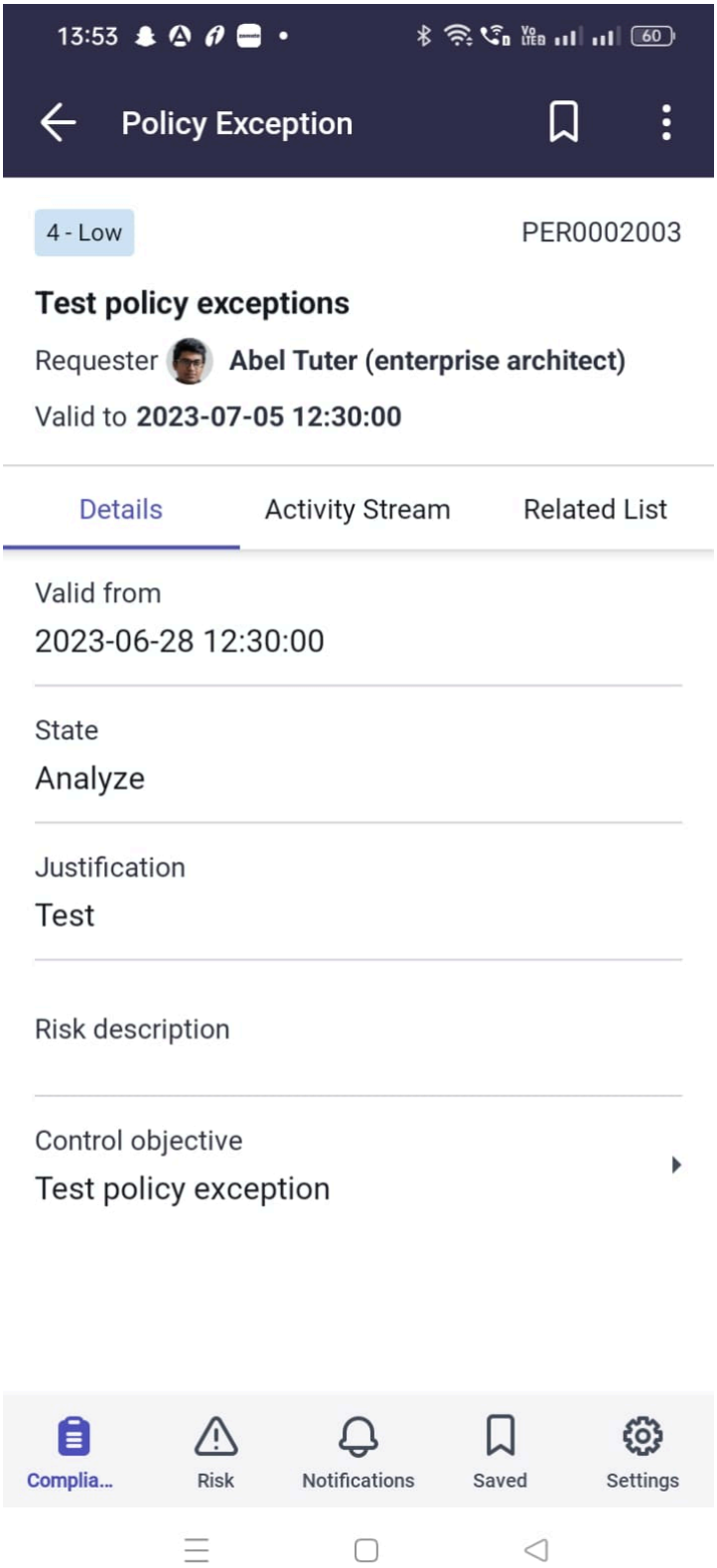
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | In the Requested extension field, tap the calendar icon to edit the date. Tap **OK** followed by the Send icon () or **Submit** to save and submit your changes. |
| Reject the extension | In the Additional comments field, enter comments. Comments are required for rejections. Tap the Send icon (  ) or **Submit** to save and submit your changes. |

8. Alternatively, with the Policy Exceptions screen displayed, tap a record on the list to open it and review more details.

   With the fields on the record displayed, choose one in the following table to continue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




| Option | Description |
|---|---|
| Details tab | With details tab selected, choose one to continue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | ◦ View the fields for details about the Policy Exception record.<br><br>If displayed, tap the **Policy** field to display a list of policies and tap an item to display the Policy record.<br><br>Tap the **Control Objective** field to display a list of control objectives. Tap an item on the list to open the record.<br><br>◦ At the top right of the screen, tap the menu icon (  ). Approve or reject the pending policy exception request, or edit it and request more information. Follow the steps described in the preceding table. If the extension request menu is displayed, follow the steps described in the preceding table to approve or reject the extension request. |
| Activity Stream tab | With the Activity Stream tab selected, choose one to continue.<br><br>◦ View work notes and additional comments. Tap the plus icon  to add a work note or attach a file.<br><br>◦ At the top right of the screen, tap the menu icon (  ). Approve or reject the pending policy exception request, or edit and request more information. Follow the steps described in the preceding table. If the extension request menu is displayed, follow the steps described in the preceding table to approve or reject the extension request. |
| Related Lists | With the Related lists tab selected, follow these steps.<br><br>**a.** Tap **Impacted Controls** to view the items on the Impacted Controls related list.<br><br>**b.** On the list that is displayed, tap an item to open the record and view more details.<br><br>At the top right of the screen, tap the menu icon (  ). Approve or reject the pending policy exception request, or edit and request more information. Follow the steps described in the preceding table. If the extension request menu is displayed, follow the steps described in the preceding table to approve or reject the extension request. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| Screen icons at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br>◦ Tap the Policy and Compliance icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br>◦ Tap **More**:<br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **Settings** followed by **Logout** to log out of the current instance. |

### Assign Policy and Compliance Management indicator tasks with the GRC Mobile application

Assign unassigned Policy and Compliance Management indicator tasks to a member of your assignment group. An indicator task is related to a Control record that is assigned to your compliance group.

#### Before you begin

Role required: GRC Compliance manager (sn_compliance.manager)

#### About this task

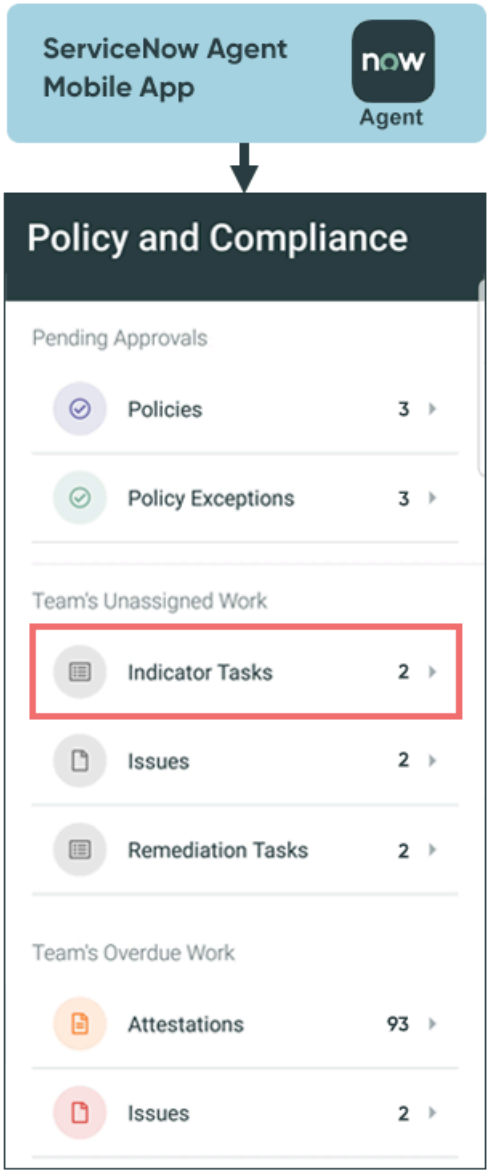
Assign a task from the list of records. Alternatively, view the details of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

#### Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Policy and Compliance screen displayed, under the section titled, `Team's Unassigned Work`, tap **Indicator Tasks**.

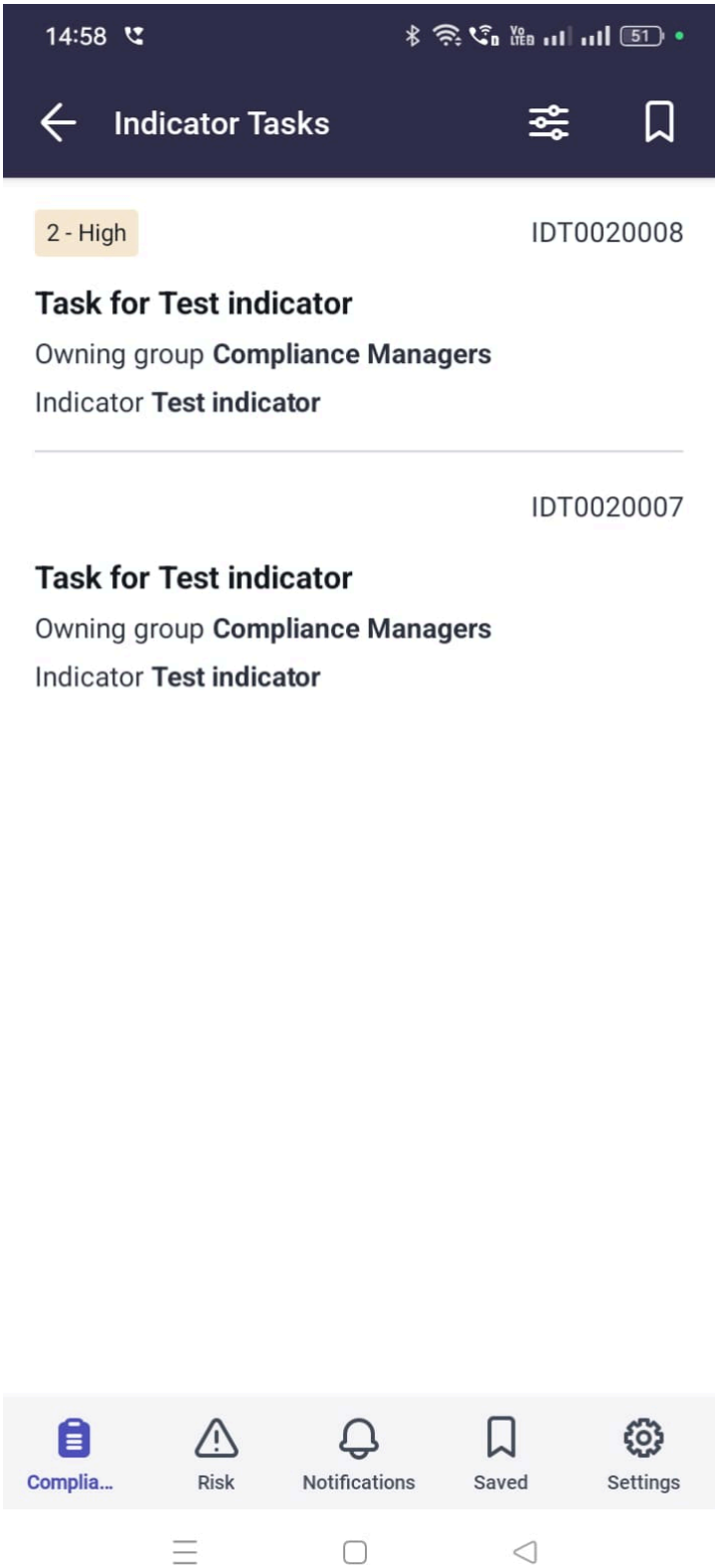
   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The Indicator Tasks screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

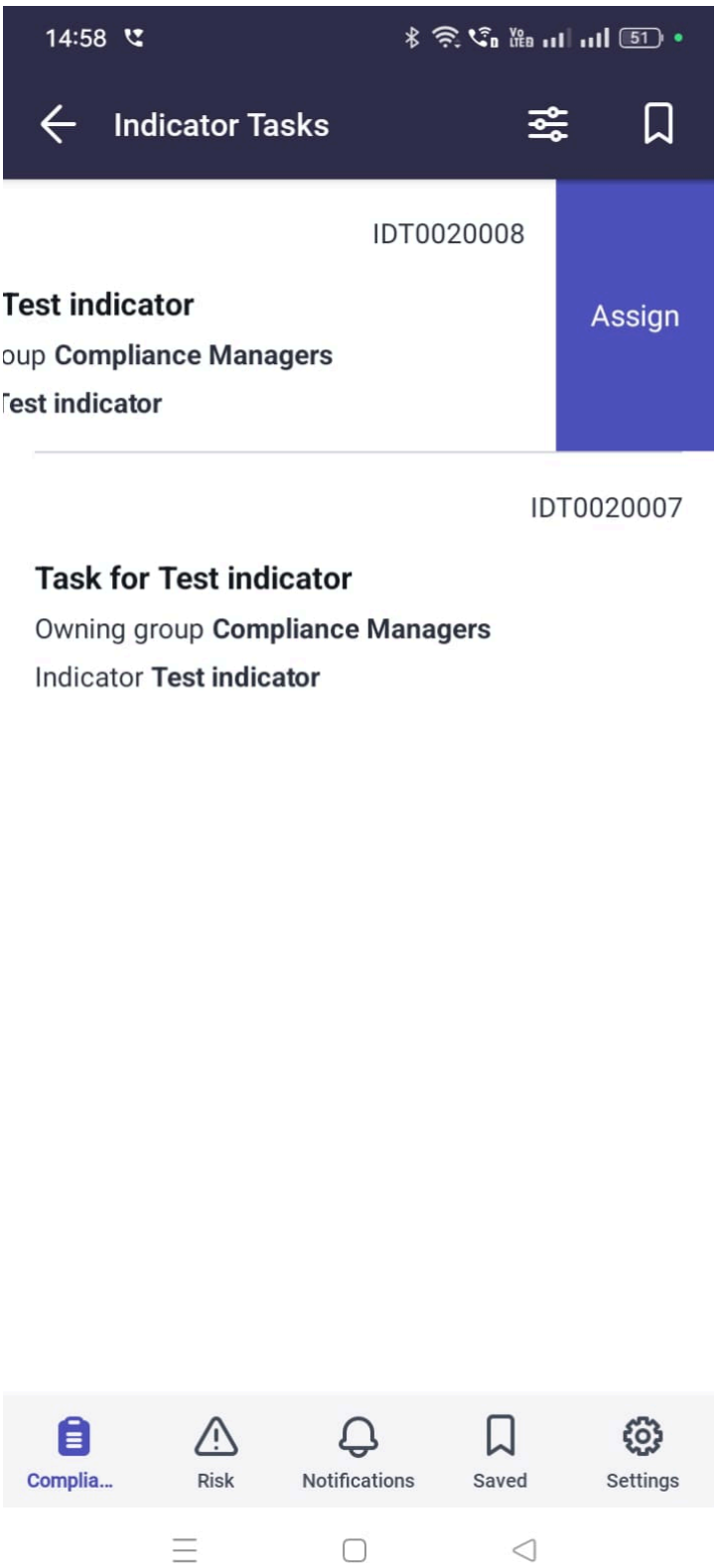



3. Optional: If you want to reduce the number of records that are displayed on the screen, see Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To assign a task directly from the list of records displayed on the Indicator Tasks screen, swipe left on a record to open the menu.



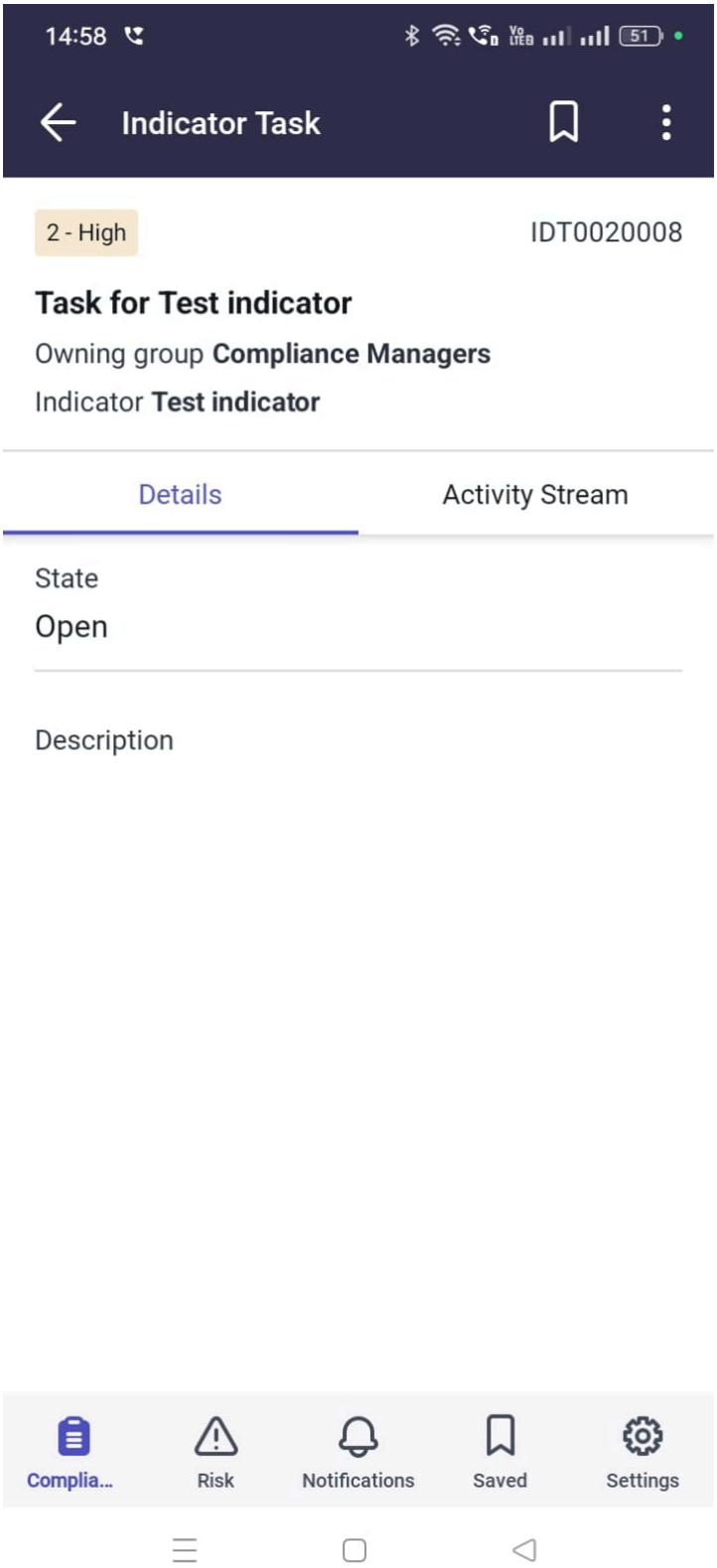

5. Tap **Assign**.
6. Tap **Assigned to**, and, on the screen that is displayed, tap a user. Alternatively, enter text in the Search field.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The name of the user is displayed on the Assign Indicator Task screen. You can assign indicator tasks to any user.

7. Tap the Send icon (  ) or **Submit** to save and submit your changes.
   After you assign the task to a user, the record is no longer displayed on the Indicator Tasks list.
8. Alternatively, to review more details, with the Assign Indicator Task screen displayed, tap a record on the list to open it.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**9.** With the fields on the record displayed, choose one in the following table to continue.

| Option | Description |
| --- | --- |
| Details tab | With the Details tab selected, view the details of the task. At the top right of the |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | screen, tap the menu icon (  ) to assign the task. On the screen that is displayed, tap a user. Alternatively, enter text in the Search field. Tap the send icon (  ) or **Submit** to save and submit your changes. |
| Activity Stream tab | With the Activity Stream tab selected, choose one to continue.<br>◦ View work notes and additional comments. Tap the plus icon (  ) to add a work note or attach a file.<br>◦ At the top right of the screen, tap the menu icon (  ) to assign the task. On the screen that is displayed, tap a user. Alternatively, enter text in the Search field. Tap the send icon (  ) or **Submit** to save and submit your changes. |
| Screen icons at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br>◦ Tap the Policy and Compliance icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br>◦ Tap **More**:<br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **Settings** followed by **Logout** to log out of the current instance. |

### Assign Policy and Compliance Management issues with the GRC Mobile application

Assign unassigned Policy and Compliance Management issues to a member of your assignment group. Navigate through the record to view more details about the Control Objective, the Control record, and Remediation Tasks associated with an issue.

#### Before you begin

Role required: GRC Compliance manager (sn_compliance.manager)

#### About this task

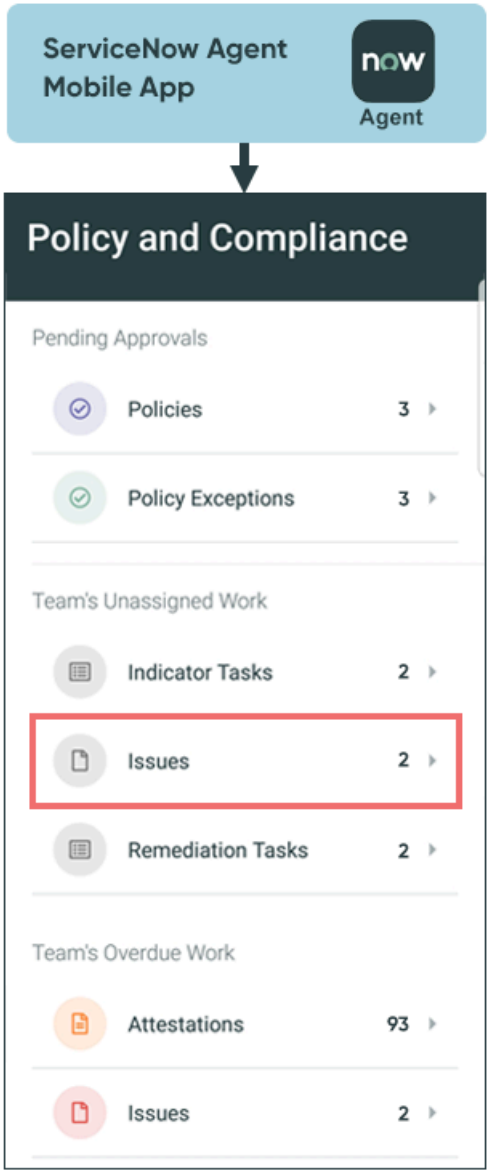
Time to complete this task: 5-10 minutes.

#### Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Policy and Compliance landing screen displayed, under the section titled, `Team's Unassigned Work`, tap **Issues**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.



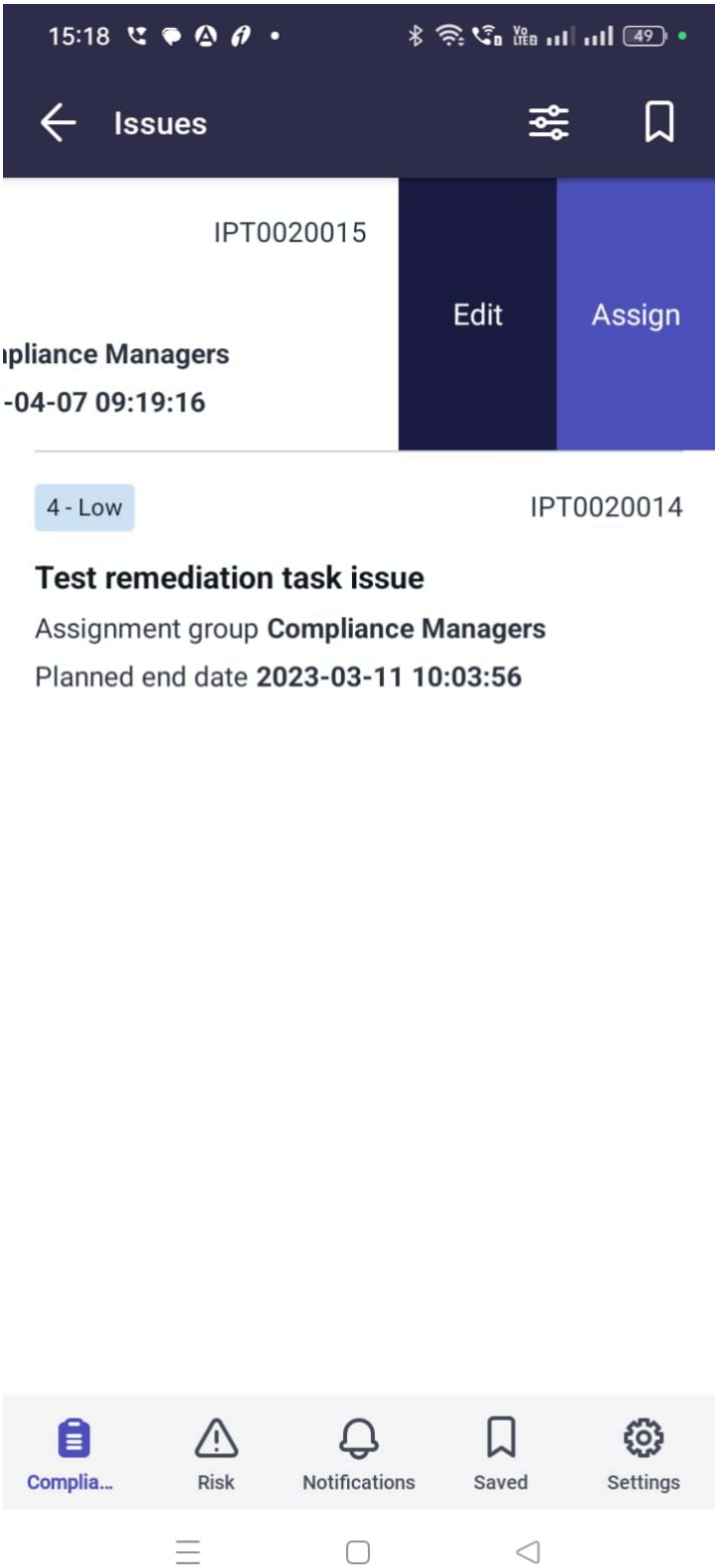

The Issues screen is displayed with a list of records.

3. Optional: If you want to reduce the number of records that are displayed on the screen, see Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

4. To edit or assign an issue directly from the list of records displayed on the Issues screen, swipe left on a record to open the menu.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**5.** In the menu that is displayed, choose one to continue.

| Option | Description |
| --- | --- |
| Edit | In the Extend by days field on the Edit Issue screen that is displayed, enter a value. This value is added to the Duration field in |

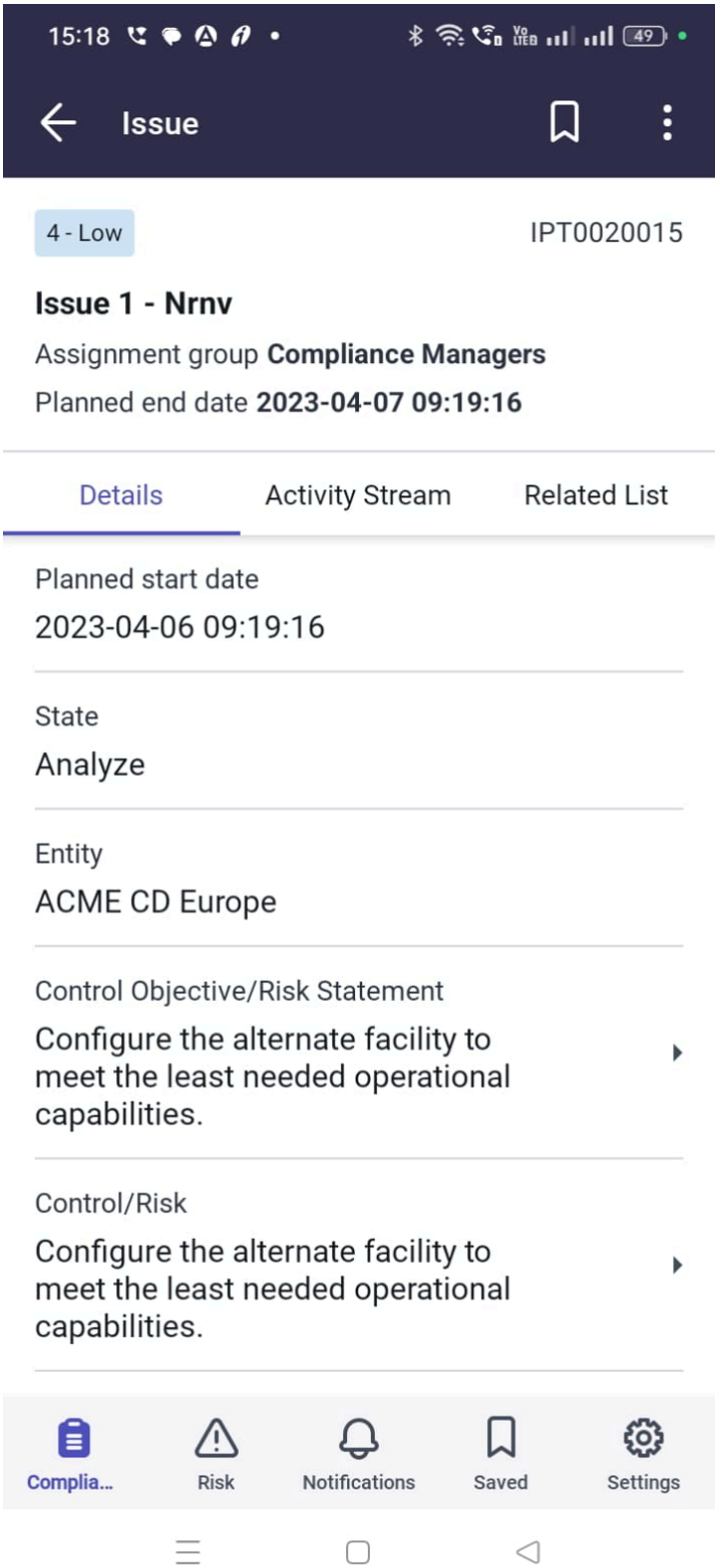
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | your Now Platform instance. Tap the Send icon () or **Submit** to save and submit your changes. |
| Assign | On the Issue Assignment screen that is displayed, tap the **Assignment Group** and **Assigned to** fields to assign the issue. |

6. Alternatively, with the Issues screen displayed, tap a record on the list to open it and view more details.

   With the fields on the issue record displayed, choose one in the following table to continue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




| Option | Description |
| --- | --- |
| Details tab | With the Details tab selected, choose one to continue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | ◦ View the fields for details about the issue, especially the planned start and end dates.<br><br>Tap the **Control Objective/Risk Statement** field to expand it. A list of records is displayed. Tap an item to display a control objective record.<br><br>Tap the **Control/Risk** field to expand it. A list of records is displayed. Tap an item on the list to open the record. With the record displayed, select the **Details** or **Activity Stream** tabs for more information.<br><br>◦ At the top right of the screen with the Issue screen displayed, tap the menu icon ( ) to edit and assign the issue. Follow the steps described in the preceding table. |
| Activity Stream tab | Choose one to continue.<br>◦ View work notes and additional comments. Tap the plus icon ( ) to add a work note or attach a file.<br>◦ At the top right of the screen, tap the menu icon ( ) to edit and assign the issue. Follow the steps described in the preceding table. |
| Related List tab | View the related lists.<br><br>**a.** Tap **Remediation Tasks** to expand the field. On the Remediation Task screen, view the items on the Remediation Tasks related list that are associated with the Issue record.<br>**b.** On the list that is displayed, tap an item to open the record and view more details about the task.<br>**c.** After your review, navigate back to the issue record and tap the menu ( ) to edit and assign the issue. Follow the steps described in the preceding table. |
| Screen icons at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br>◦ Tap the Policy and Compliance icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | ◦ Tap **More**:<br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **Settings** followed by **Logout** to log out of the current instance. |

### Assign Policy and Compliance Management remediation tasks with the GRC Mobile application

Assign an unassigned remediation task to a member of your group. Edit the fields including the **Extend by days** field. Navigate through the record to view more details about the Control Objective, the Control record, and the Issues associated with a Remediation Task.

#### Before you begin

Role required: GRC Compliance manager (sn_compliance.manager)

#### About this task

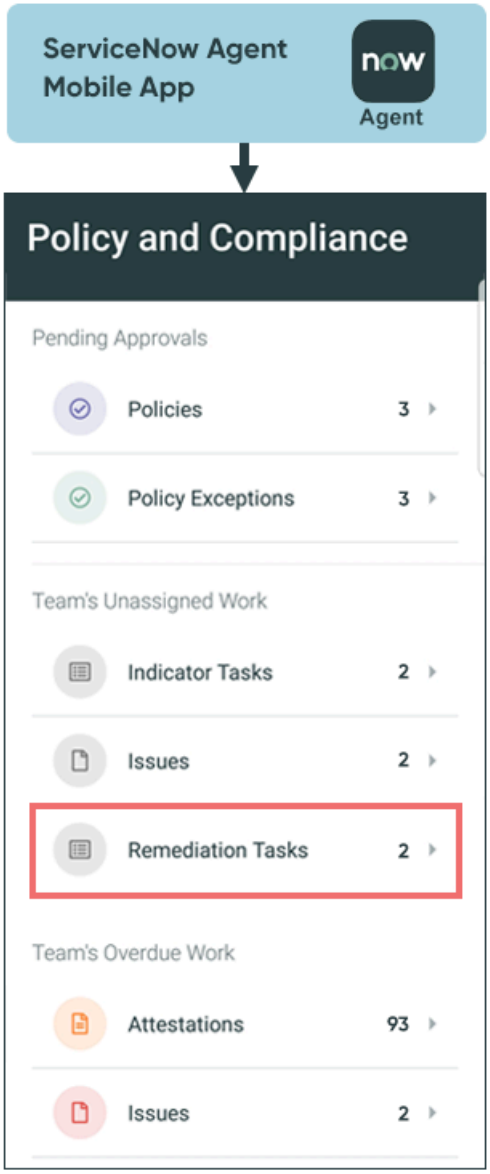
Edit or assign an unassigned remediation task directly from the list of records. Alternatively, view the details of the record prior to assignment or add a work note. Time to complete this task: 5-10 minutes.

#### Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Policy and Compliance landing screen displayed, under the section titled, `Team's Unassigned Work`, tap **Remediation Tasks**.

   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The Remediation Tasks screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

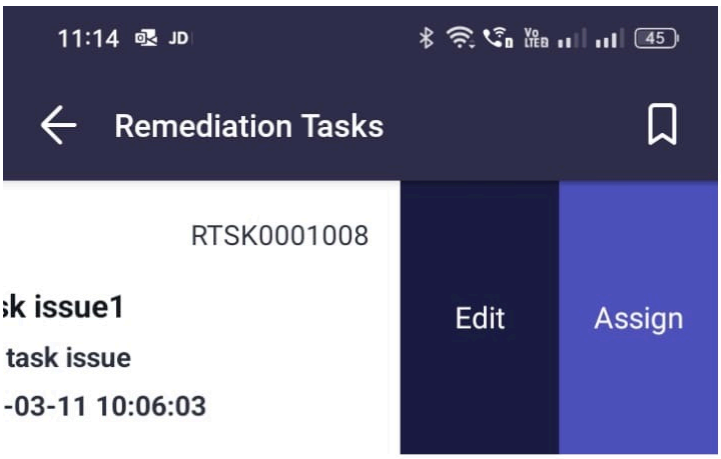



3. Optional: See Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To edit or assign a task directly from the list of records displayed on the Remediation Tasks screen, swipe left on a record to open the menu.

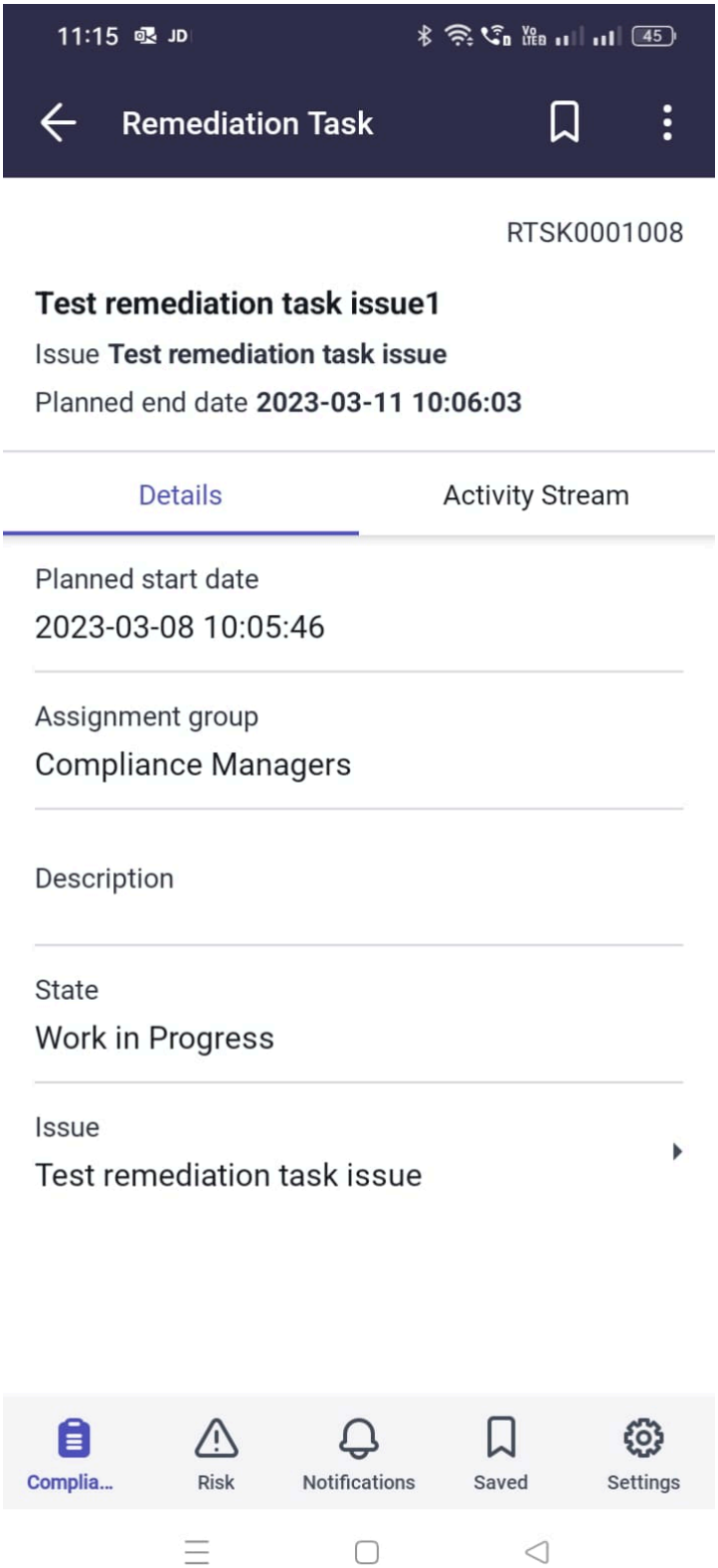



5. In the menu that is displayed, choose one to continue.

| Option | Description |
|---|---|
| Edit | In the Extend by days field on the Edit Remediation Task screen that is displayed, enter a value. This value is added to the Duration field in your Now Platform instance.<br><br>To assign the remediation task, tap the Assigned to field and tap a name. Alternatively, enter a user name in the search field.<br><br>Tap the Send icon ( ) or **Submit** to save and submit your changes. |
| Assign | On the Issue Assignment screen that is displayed, tap the **Assignment Group** and **Assigned to** fields to assign the issue. |

6. Alternatively, with the Remediation Tasks screen displayed, tap a record on the list to open it and review more details.
7. With the fields on the issue record displayed, choose one in the following table to continue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




| Option | Description |
| --- | --- |
| Details tab | With the Details tab selected, choose one to continue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | ◦ View the fields for details about the issue, especially the planned start and end dates.<br><br>Tap the Issue field to expand it. On the Issue screen, a list of records is displayed. Tap an item to display more details about the Control Objective and Control/Risk.<br><br>◦ Navigate back to the record on the Remediation Task screen and tap the menu icon ( ) to assign or edit the issue. Follow the steps described in the preceding table. |
| Activity Stream tab | With the Activity Stream tab selected, choose one to continue.<br><br>◦ View work notes and additional comments. Tap the plus icon ( ) to add a work note or attach a file.<br><br>◦ At the top right of the screen, tap the menu icon ( ) to edit and assign the issue. Follow the steps described in the preceding table. |
| Screen icons at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br><br>◦ Tap the Policy and Compliance icon to return the landing screen.<br><br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br><br>◦ Tap **More**:<br><br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br><br>▪ Tap **Settings** followed by **Logout** to log out of the current instance. |

### Reassign overdue Policy and Compliance Management attestations with the GRC Mobile application

Reassign overdue attestations to a member of your assignment group.

#### Before you begin

Role required: GRC Compliance manager (sn_compliance.manager)

#### About this task

Reassign a record from the list. Alternatively, view the details of the record prior to reassignment. Time to complete this task: 5-10 minutes.

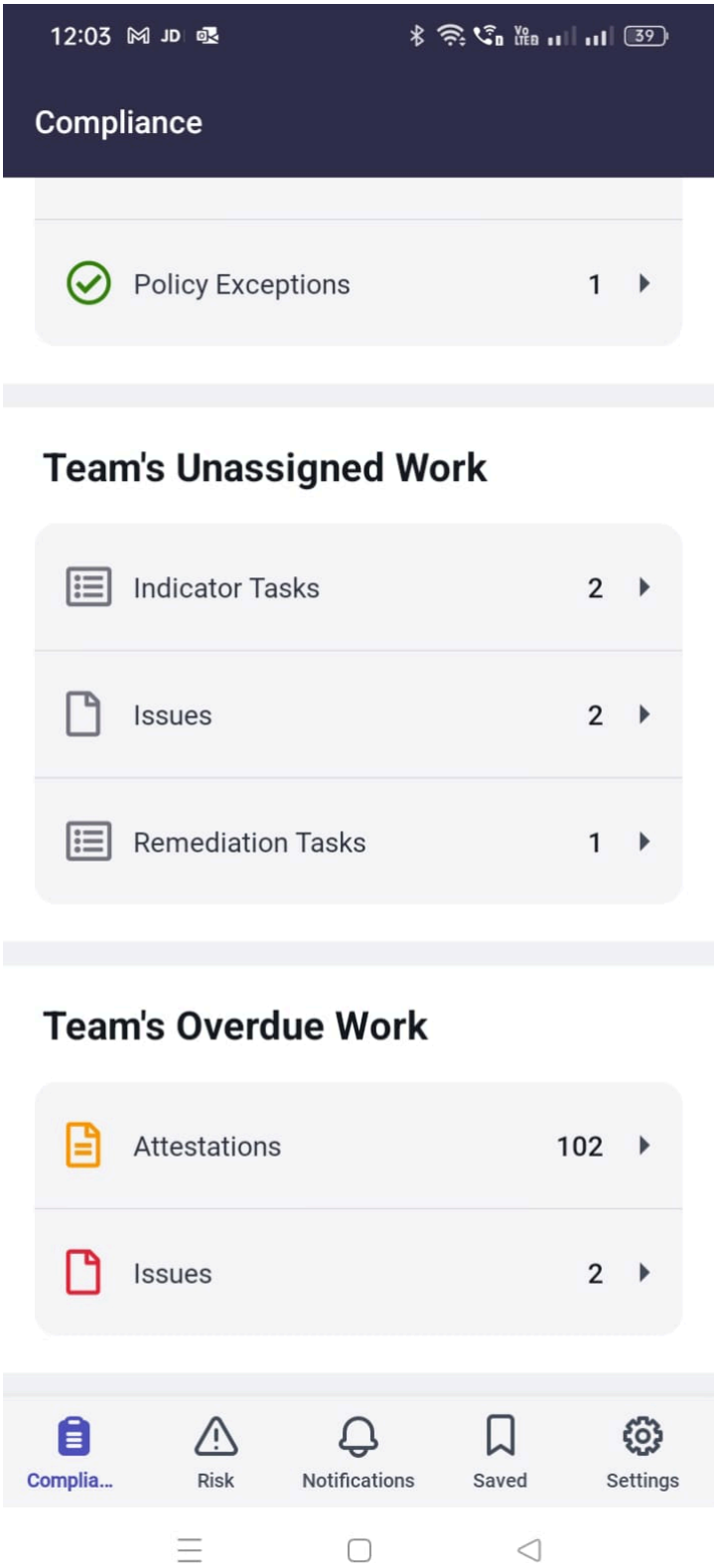
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Policy and Compliance screen displayed, under the section titled, `Team's Overdue Work`, tap **Attestations**.

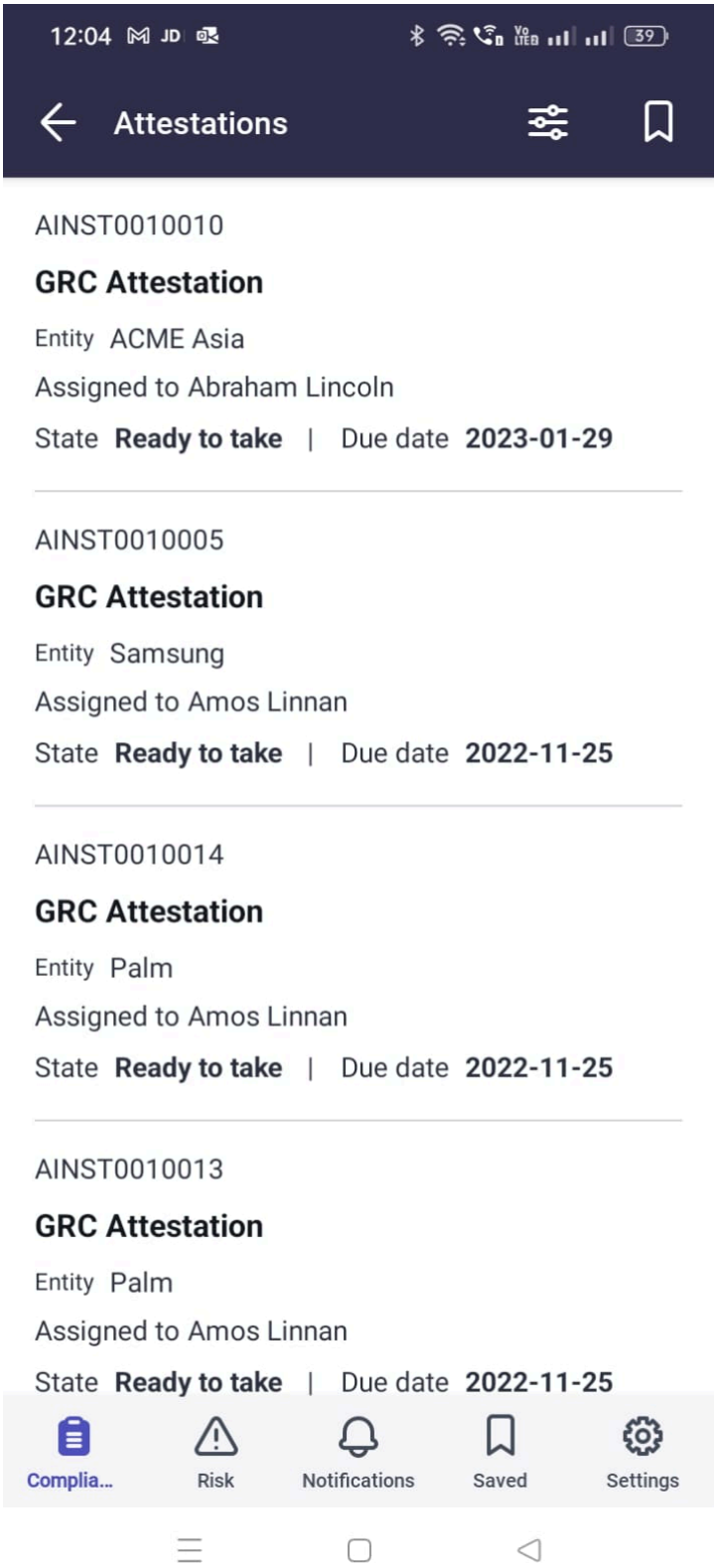
   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The Attestations screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

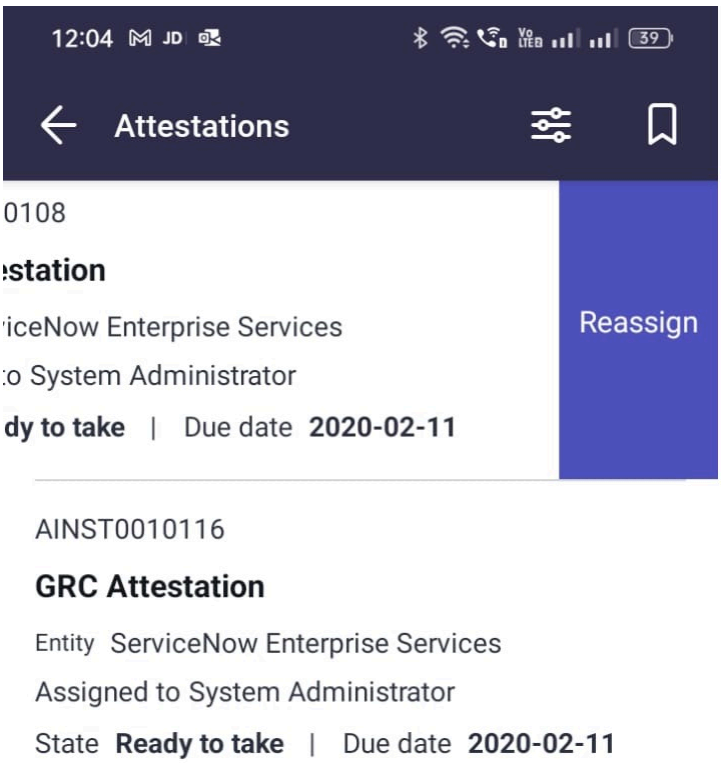



3. Optional: See Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

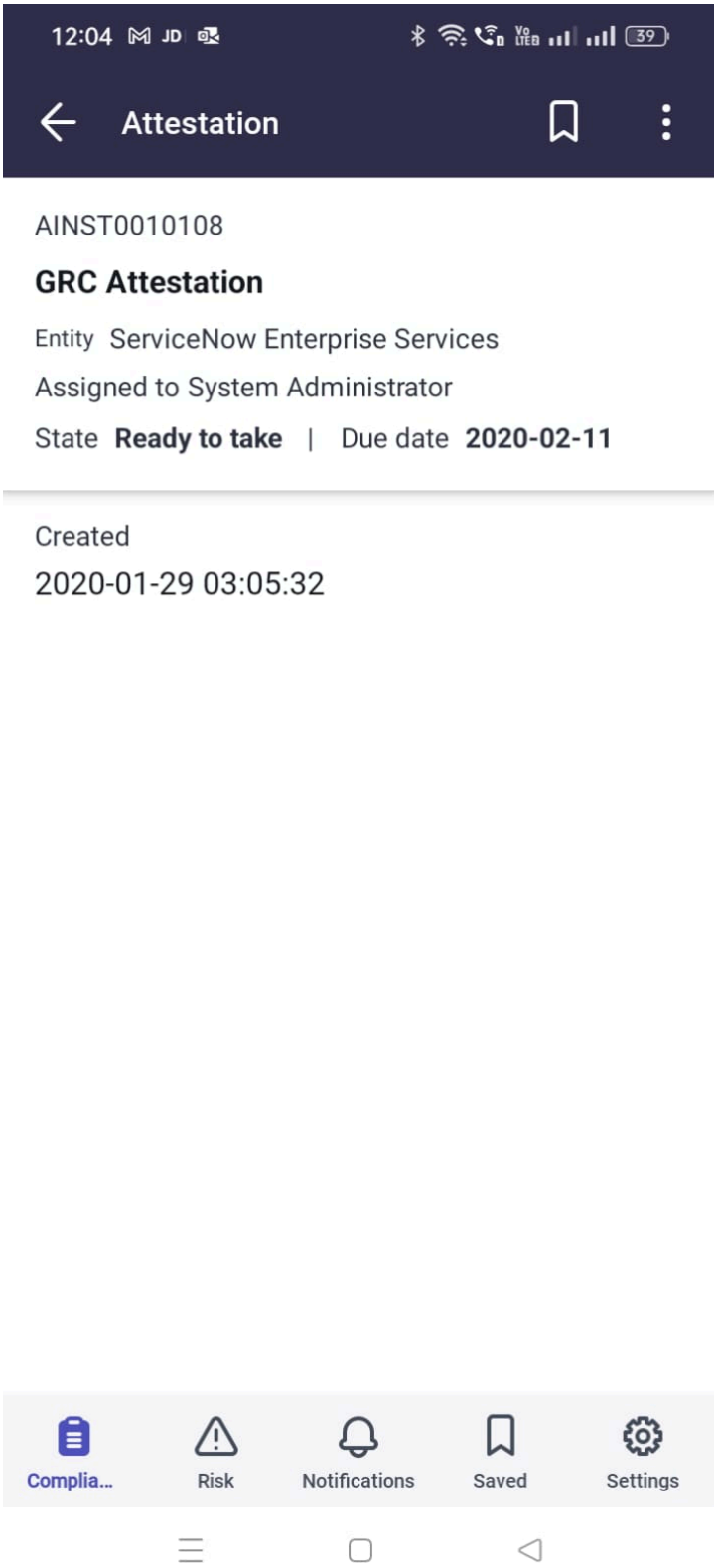
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To reassign an attestation directly from the list of records displayed on the Attestations screen, swipe left on a record to open the menu.




5. Tap **Reassign** and followed by the **Assigned to** field.
6. Tap a user name, or, alternatively, enter a name in the search field.
7. Tap the Send icon () or **Submit** to save and submit your changes.
8. Alternatively, with the Attestation screen displayed, tap a record on the list to open it and view more details.
9. Choose one from the following table to continue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




| Option | Description |
|---|---|
| Tap the top menu icon | Tap the menu icon ( ) to reassign the attestation. |
| Screen icons at the bottom of the screen. | On the bottom of the screen, choose one to continue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | ◦ Tap the Policy and Compliance icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br>◦ Tap **More**:<br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **Settings** followed by **Logout** to log out of the current instance. |

### Reassign overdue Policy and Compliance Management issues with the GRC Mobile application

Reassign overdue issues that are assigned to your assignment group. Navigate through the record to view more details about the Control Objective, the Control record, and Remediation Tasks that are associated with an overdue issue.

#### Before you begin

Role required: GRC Compliance manager (sn_compliance.manager)

#### About this task

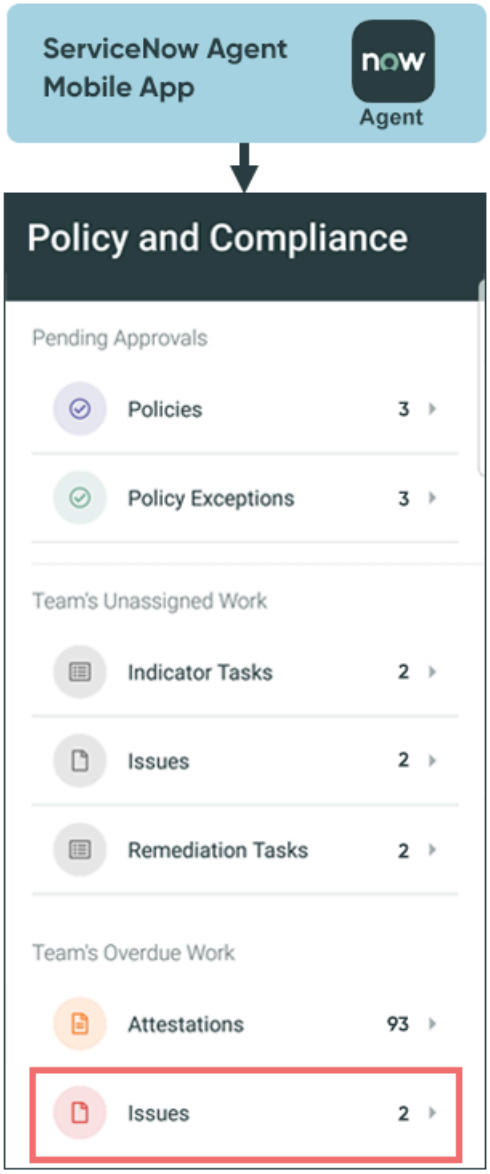
Edit or reassign an issue directly from the list of records. Alternatively, add a work note or navigate through the record to view more details prior to reassignment. If an issue is not assigned to your assignment group, it is not displayed on this list. Time to complete this task: 5-10 minutes.

#### Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Policy and Compliance screen displayed, under the section titled `Team's Overdue Work`, tap **Issues**.

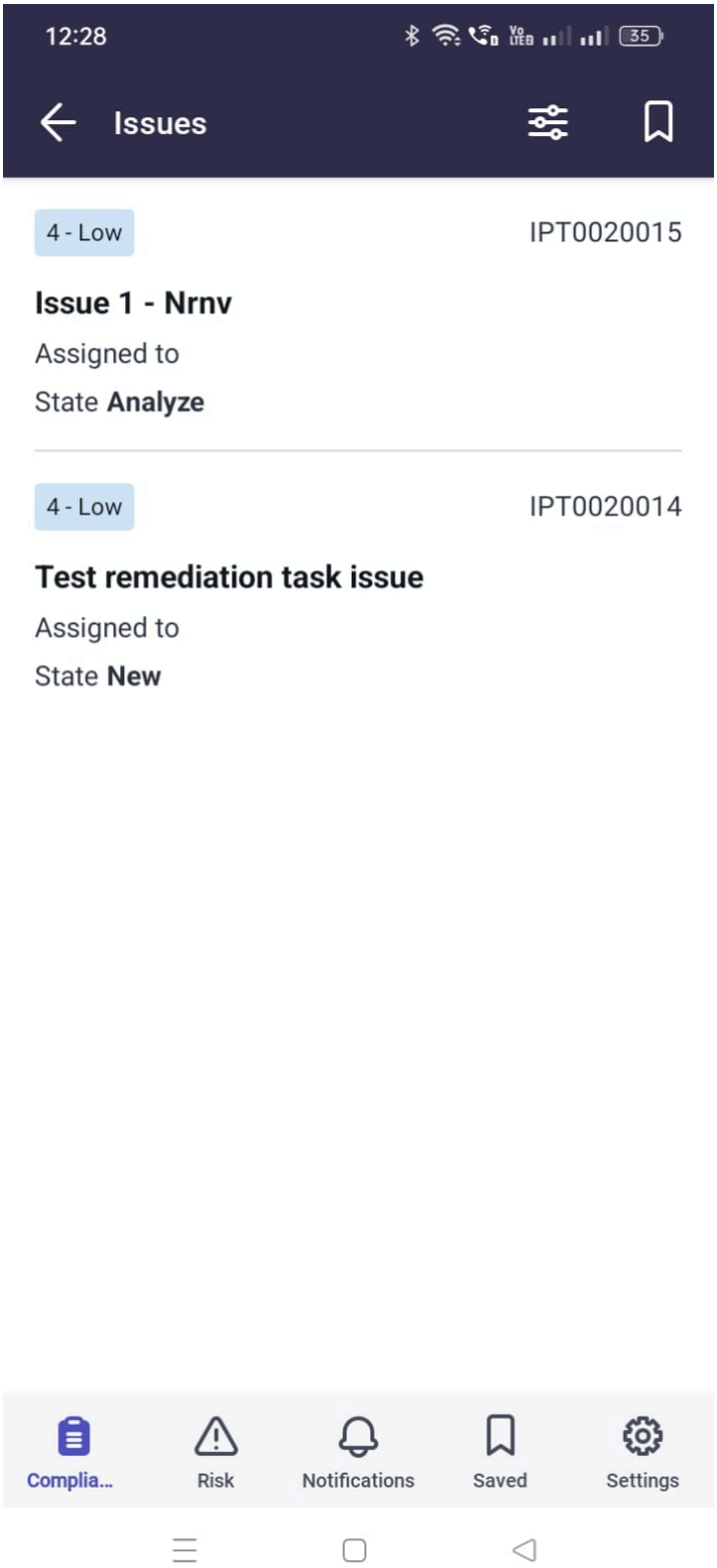
   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The Issues screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

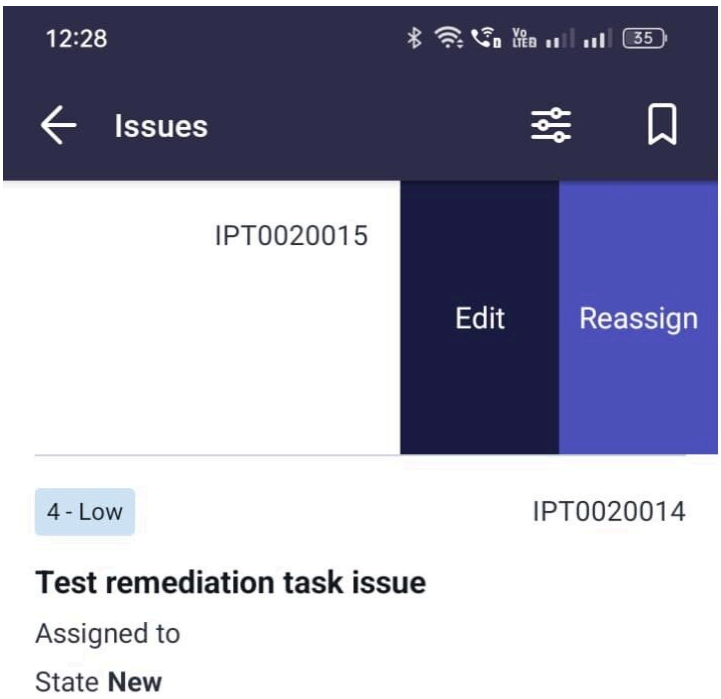



3. Optional: See Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To edit or reassign an issue directly from the list of records displayed on the Issues screen, swipe left on a record to open the menu.

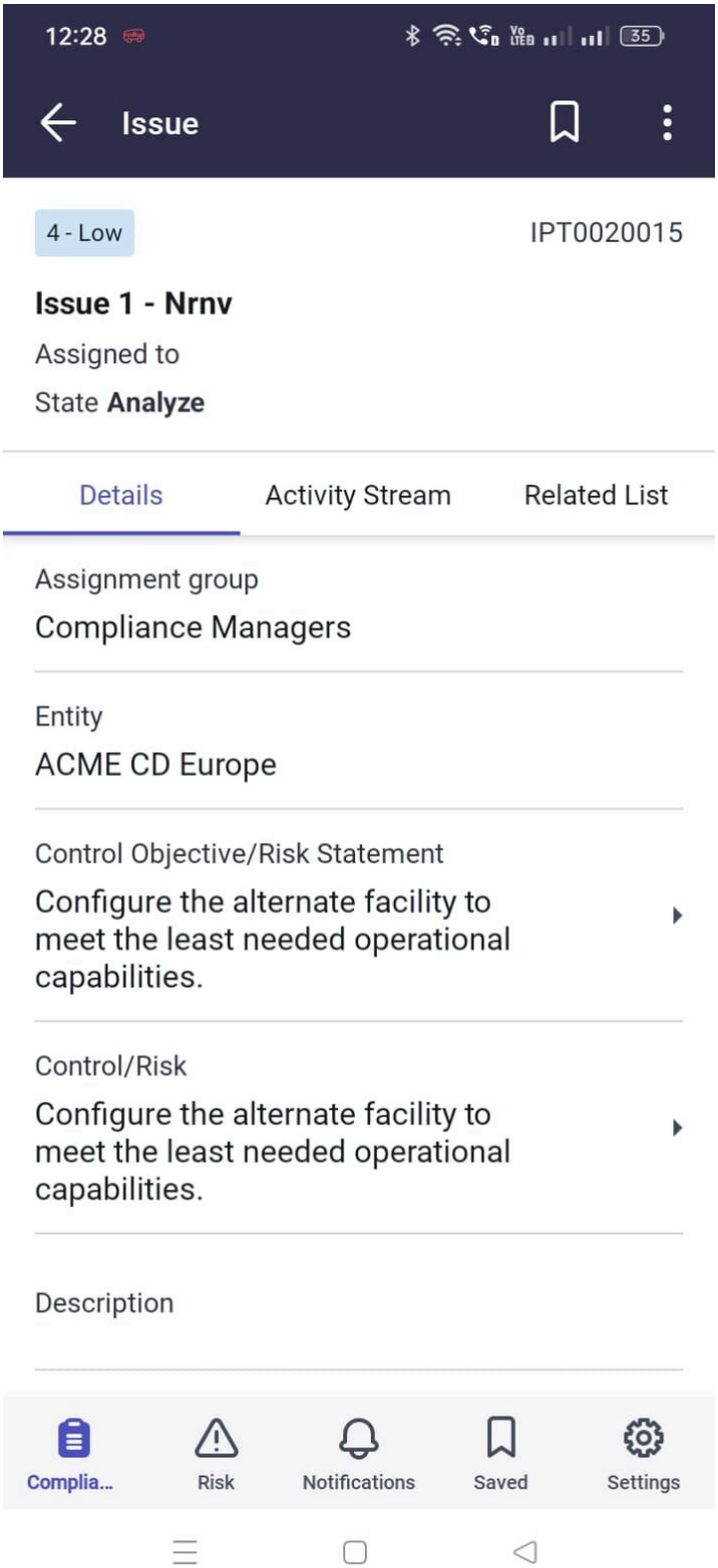



5. In the menu that is displayed, choose one to continue.

| Option | Description |
|---|---|
| Edit | In the Extend by days field on the Edit Issue screen that is displayed, enter a value. This value is added to the Duration field in your Now Platform instance. Tap the Send icon ( ) or **Submit** to save and submit your changes. |
| Reassign | On the Issue Assignment screen that is displayed, tap the Assignment Group and Assigned to fields to reassign the issue. Tap the Send icon ( ) or **Submit** to save and submit your changes. |

6. Alternatively, with the Issues screen displayed, tap a record on the list to open it and view more details.
7. With the fields on the issue record displayed, choose one in the following table to continue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




| Option | Description |
| --- | --- |
| Details tab | With the Details tab selected, choose one to continue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | ◦ View the fields for details about the issue, especially the planned start and end dates.<br><br>Tap the **Control Objective/Risk Statement** field to expand it. A list of records is displayed. Tap an item to display the control objective record.<br><br>Tap the **Control/Risk** field to expand it. A list of records is displayed. Tap an item on the list to open the record. With the record displayed, select the **Details** or **Activity Stream** tabs for more information.<br><br>◦ Navigate back to the record and tap the menu icon ( ) to edit and reassign the issue. Follow the steps described in the preceding table. |
| Activity Stream tab | With the Activity Stream tab selected, choose one to continue.<br>◦ View work notes and additional comments. Tap the plus icon ( ) to add a work note or attach a file.<br>◦ At the top right of the screen, tap the menu icon ( ) to edit and reassign the issue. Follow the steps described in the preceding table. |
| Related List tab | With the Related List tab selected, follow these steps.<br><br>**a.** Tap **Remediation Tasks** to expand the field. On the Remediation Task screen, view the items on the Remediation Tasks related list that are associated with the Issue record.<br>**b.** After your review, navigate back to the record on the Issue screen and tap the menu icon ( ) to edit and reassign the issue. Follow the steps described in the preceding table. |
| Screen icons at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br>◦ Tap the Policy and Compliance icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br>◦ Tap **More**: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | ▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **Settings** followed by **Logout** to log out of the current instance. |

### Filter records with the GRC Mobile application

Set additional filters to limit the number of records that are displayed on a screen. Filtering records in the mobile app works like filtering with a condition builder on the Now Platform.

#### Before you begin
Role required: Compliance manager (sn_compliance.manager)

#### About this task
Time to complete this task: 5 minutes.

#### Procedure
1. To further refine your search results, or to enter additional filter criteria on any list of records that is displayed, tap the filter icon ( ).
2. With the Filters screen displayed, tap a field to expand it.
3. From the options that are displayed, tap the check box or tap an option for your filter. For many of the filters, you can select more than one option.
4. Tap the Back icon ( ) or **DONE** to save your changes to a field.
   The criteria you chose are displayed on the Filters screen. The number of records that match your criteria is also displayed at the top of the screen. Tap **Clear** or **RESET** to remove any filters and restore the default setting.
5. Optional: Repeat steps 1 - 4 with the Filters screen displayed to continue setting your filter criteria.
6. Tap the intersection union after you set all criteria to create AND conditions. ).
   Alternatively, tap the union icon ( ) to create OR conditions.
7. After you have added all the criteria you want, with the Filters screen displayed, tap **DONE**.
   On the screen, only the records that match your filter criteria are displayed.

#### What to do next
View the records that are displayed after your search for more details.

### Create a GRC article template

Policy and Compliance managers can create templates for policy article publishing.

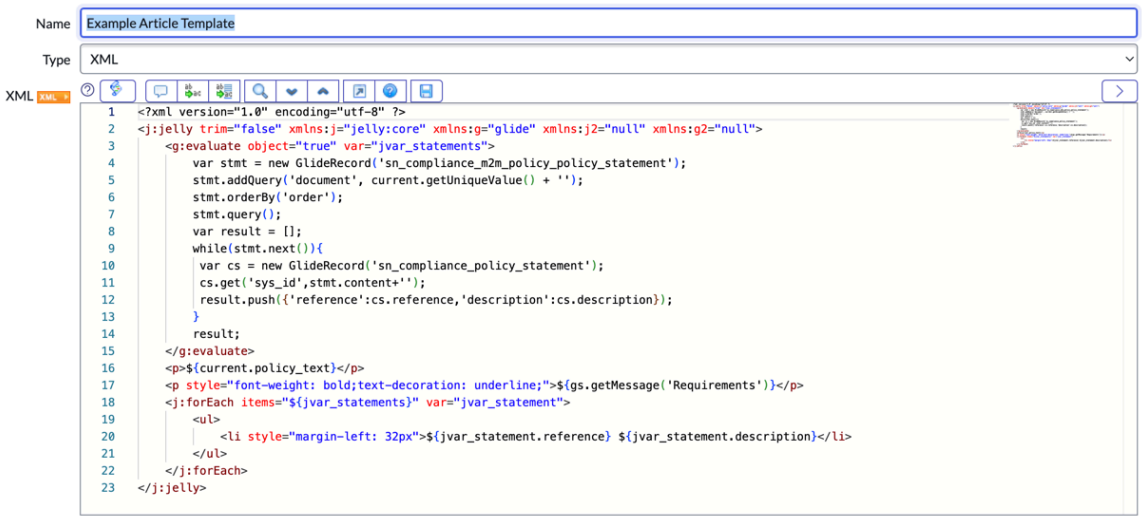
#### Before you begin
Role required: sn_compliance.developer

#### Procedure
1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Article Templates**.
2. Click **New**.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Authority Document

| Field | Description |
|---|---|
| Name | Name of the article template. |
| Type | ◦ Script<br>◦ HTML<br>◦ XML |
| Script | The script code. This field depends on the **Type** field. |
| HTML | The HTML code. This field depends on the **Type** field. |
| XML | The XML code. This field depends the **Type** field. |
| Is default | Option to indicate that this template is used as the default template for all KB articles. |




4. Click **Submit**.

## Create or deactivate a citation

Usually, authority documents, citations, and control objectives are downloaded from a third-party provider. However, citations can be created manually from an authority document. The **Active** option in a citation indicates whether the citation is active or inactive.

### Before you begin

Role required: sn_compliance_admin or sn_compliance_manager

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Authority Documents**.
2. Open an authority document.
3. In the **Citations** related list, click **New**.
4. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Citation form

| Field | Description |
|---|---|
| Name | User-defined name that identifies this citation. |
| Source | Source of the policy. For example, if the statement is from a third-party provider, indicate which one. |
| Source ID | Unique identification number used by the source to catalog this authority document. |
| Reference | Content reference. |
| Type | Type of citation created. Optional field not used for any processing. Use the value in this field in reports or to query for records of a specific type.<br>◦ Core Topic<br>◦ Process<br>◦ Control Objective<br>◦ Control<br>◦ Supporting information |
| Authority document | Name of the parent authority document for this citation. When you create citations from the authority document form, the system completes this field automatically. |
| Active | Option that indicates if a policy is active. A policy is marked active if it is not in the **Draft** or **Retired** state. To deactivate a citation, clear the check box marked **Active**. |
| Parent | References the parent content. |
| Description | Description of the citation. |

5. In the Settings related list, select the **Functional domain** field.
6. Select a domain.
   Only the citations specific to the selected domain appear in your application.

## Set notification properties

After an acknowledgement request has been sent to an audience, different reminder notifications are sent based on the timeliness and state of the response. Properties allow you to configure the notifications.

These properties are available for Policy and Compliance Management.

**Note:** Navigate to **Policy and Compliance > Administration > Properties**.

### Properties for Policy and Compliance Management

| Property | Description |
|---|---|
| Specify how many days after due date to send Policy Acknowledge summary notification. | The number of days after an acknowledgement due date has passed before a Policy Acknowledge summary notification is sent. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Properties for Policy and Compliance Management (continued)**

| Property | Description |
|---|---|
| States for which the control is active (the first state is the default active state) | States of the control in which it is considered active. The first state in the list is the default active state. |
| Number of days after Policy Acknowledgement Due Date to send overdue notification. | The number of days after an acknowledgement due date has passed before an overdue notification is sent. |
| Send a summary of the Policy Acknowledge after its due date. Use property sn_compliance.policy_ack_after_due_summary_timer to specify how many days after due date to send notification. | Select Yes to send a Policy Acknowledge summary notification after the days specified in the **Specify how many days after due date to send Policy Acknowledge summary notification** property has elapsed.<br><br>For example, if the property is set to 1 day, the notification is sent when the acknowledgement is 1 day late. |
| Send a summary of the Policy Acknowledge before its due date. Use property sn_compliance.policy_ack_before_due_summary_timer to specify how many days before due date to send notification. | Select Yes to send a Policy Acknowledge summary notification prior to the number of days specified in the **Specify how many days after due date to send Policy Acknowledge summary notification** property is reached.<br><br>For example, if the property is set to 1 day, the notification is sent 1 day before the due date. |
| Repeat the Policy Acknowledgement overdue notification daily | Select Yes to repeat the overdue notification on a daily basis until it is completed. |
| Number of days before Policy Acknowledgement Due Date to send reminder notification. | The number of days prior to the acknowledgement due date to begin sending reminder notifications. |
| Repeat the Policy Acknowledgement Due Date reminder daily until Policy Acknowledgement is due | Select Yes to send reminder notifications on a daily basis starting on the day determined by your setting in the **Number of days before Policy Acknowledgement Due Date** to send reminder notification property.<br><br>For example, if you select Yes in this property and the due date occurs in 7 days, and you specified 3 days in the previous |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Properties for Policy and Compliance Management (continued)**

| Property | Description |
|---|---|
| | property, reminder notifications begin in 3 days and repeat daily. |
| Specify how many days before due date to send Policy Acknowledge summary notification. | The number of days prior to the due date to send the Policy Acknowledge summary notification. |

### Set up GRC Virtual Agent for requesting an exception to a policy or a control objective

Set up the Governance, Risk, and Compliance Virtual Agent to request an exception to a policy or a control objective from the Service Portal.

#### Before you begin

Role required: sn_risk.admin

Customers must have the following plugins activated for setting up the GRC Virtual Agent:

- Glide Virtual agent (com.glide.cs.chatbot) activated with a valid license.
- GRC Policy and Compliance Management.

#### About this task

A virtual agent chatbot enables customers to request an exception. The chatbot assists the customers by saving their time. The information exchanged during the conversation flow enables the chatbot to fulfill a user request or assist a user in completing a task.

#### Procedure

1. Navigate to **All** > **Service Portal** > **Service Portal Configuration**.
2. Click **Page Editor**.
3. In the search field, type `Index`.
4. Click **Service Portal index**.
5. At the top of the page, click **Edit Service Portal (index) page in Designer**.
6. In the Filter Widget search field, type `Virtual Agent Service Portal Widget` and drag and drop the widget anywhere on the screen.

   You can see the chat icon at the bottom-right of the screen.

### Allow policy exception requests from other applications

Starting with Version 10.1, you can leverage new policy exception capabilities in Policy and Compliance Management from within other applications.

Requests are routed through multiple approvals based on risk rating, policy, and control objective associated with an exception. Compliance and risk teams obtain better visibility with respect to exceptions raised for vulnerabilities.

**Note:** Starting with Version 10.1, if you have installed Version 10.3 of the Vulnerability Response application, you can request policy exceptions using the GRC policy exception management capability inherent in the Policy and Compliance Management application. For details, see Policy Exception Integration with Vulnerability Response.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Before allowing other applications to leverage the policy exception capabilities of Policy and Compliance Management, you must first add the application to the Integration Registry and then perform some preliminary setup.

### Configure policy exceptions from other applications

Before you can request policy exceptions from applications other than Policy and Compliance Management, you must add a UI action for making the request and, optionally, create a new list view to see policy exception target records on the Policy Exception form.

#### Before you begin

Role required: sn_compliance.manager, ui_action_admin or admin

The GRC business user (sn_grc.business_user) or business user – lite (sn_grc.business_user_lite) is the minimum required role to raise a policy exception from an upstream application.

#### About this task

Starting with Version 10.1 of Policy and Compliance Management, if you have installed Version 10.3 of the Vulnerability Response application, you can request policy exceptions using the GRC policy exception management capability inherent in the Policy and Compliance Management application. The procedure below is not necessary requesting policy exceptions from Vulnerability Response as the UI action is automatically installed.

#### Procedure

1. Navigate to **All** > **System Definition** > **UI Actions**.
2. Select the table on which you want to create the UI action.
3. Click **New**.
4. Create a new UI action with the following parameters:
   - **Name**: Request policy exception
   - **Show update** check box: Selected.
   - **Form button** check box: Selected.
   - **Onclick**: Type the `popupDispList()` function call.

     **Note:** This field is available only when **Client** option is selected.

   - **Condition**: Apply any conditions you require.
   - **Script**: Enter this script:

```
function popupDispList(){


 ScriptLoader.getScripts(['sn_compliance.PolicyExceptionUtils.jsdbx'],
 function() {


 sn_compliance.PolicyExceptionUtils.createPolicyException('incident');

             });
```

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

```
}
```

**Note:** The argument for the `createPolicyException` function varies based on the integration.

5. Save the UI action.
6. To create a new list view to see policy exception target records on the Policy Exception form, see KB0783018.

### Register other applications to request policy exceptions

Enable other applications to request policy exception from any table such as Problem or Incident and so on. The applications must be added and configured in the Integration Registry.

#### Before you begin

Role required: sn_compliance.manager
The GRC business user (sn_grc.business_user) or business user – lite (sn_grc.business_user_lite) is the minimum required role to raise a policy exception from an upstream application.

#### About this task

Starting with the New York release, users from any ServiceNow application can request for policy exceptions using (GRC)'s policy exception management capability. For example, users can request policy exception for a problem related to a group of incidents that cannot be resolved for a specific duration. To be able to request policy exception, you must register the application for policy exception and create a UI action for requesting policy exception, unless one is provided with the ServiceNow application.

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policy Exceptions** > **Integration Registry**.
2. Click **New**.
3. On the form, fill in the fields.

**Policy Exception Integration Registry form**

| Field | Description |
|---|---|
| Name | Enter a name of the registry entry. |
| Policy exception target table | Select the table on which a policy exception will be applied. |
| Exception applied on | Target record on which the exception is applied. The options are:<br>◦ One target record: Specific target record on which the exception is applied. Select the assessed object in the Compliance data source registry.<br>◦ All target records: All target records on which the exception is applied. Select the policy exception target table on which the exception is applied. |
| Source type | Auto-populates **Controls** if the **Exception applied on** is **One target record**. Auto-populates **Control objective** if the **Exception applied on** is **All target records**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Policy categories | Select one or more categories for filtering policies. For example, if you select the Vulnerability Response category, and are requesting an exception using that application, the list of all policies is filtered by that category, saving you time. For more information, see Define policy categories. |
| **Entity Mapping** | |
| Relationship | Select **Reference field** when the entity is a field in the Policy Exception [sn_compliance_policy_exception] table.<br><br>Select **Related list** when the entity is in a related list of the Policy Exception table. |
| Entity field | Enter the name of the field that points to the Entity [sn_grc_profile] table.<br><br>This field displays only if you selected **Reference field** as the **Relationship**. |
| Mapping table | Select the table that establishes a relationship between the Policy Exception table and the Entity table.<br><br>This field displays only if you selected **Related list** as the **Relationship**. |
| Policy exception target field | Select the field in the mapping table that points to the Policy Exception table.<br><br>This field displays only if you selected **Related list** as the **Relationship**. |
| Entity field | Enter the name of the field in the mapping table that points to the Entity table. |
| **Request Source**<br><br>**Note:** The fields in this section are needed only if you are requesting a policy exception from a table other than the Policy Exception Target table. | |
| Table | Select the table that contains the records from which the policy exception will be requested. |
| Relationship | Select **Reference field** when the entity is a field in the Policy Exception [sn_compliance_policy_exception] table. Select **Related list** when the entity is in a related list of the Policy Exception table |
| Request source field | Select the field that points to the request source table.<br><br>This field displays only if you selected **Reference field** as the **Relationship** field in the **Request Source** section. |
| Mapping table | Select the table that establishes a relationship between the Policy Exception table and the Entity table.<br><br>This field displays only if you selected **Related list** in the **Relationship** field in the **Request Source** section. |
| Policy exception target field | Select the field in the mapping table that points to the Policy Exception table. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | This field displays only if you selected **Related list** in the **Relationship** field in the **Request Source** section. |
| Request source field | Select the field in the mapping table that points to the request source table.<br><br>This field displays only if you selected **Related list** in the **Relationship** field in the **Request Source** section. |
| **Questionnaire Details** | |
| Exception questionnaire | Select a questionnaire template to generate a questionnaire for the requested policy exception. For more information, see Create an exception questionnaire. |

4. Save the record.

   The Reason Choices related list appears.

> **Note:** The Reason Choices are available to the person who requests a policy exception to explain the purpose of the request. So define reasons that apply to your specific situation. For more information, see Define policy exception reason choices.

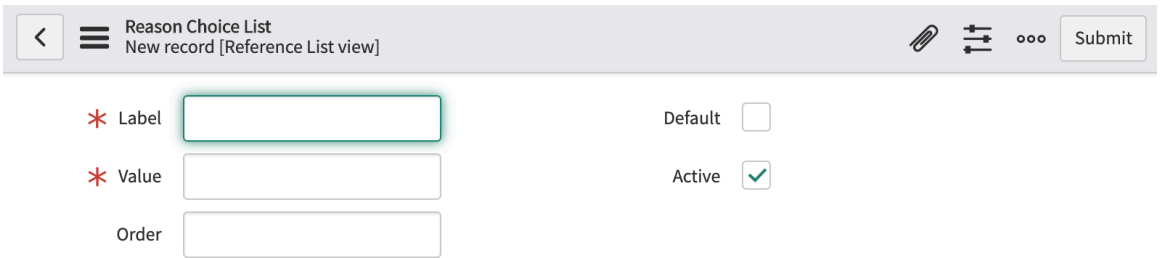
### Define policy exception reason choices

You can define reason choices to be available to any user who requests an exception.

**Before you begin**
Role required: sn_compliance.manager

**Procedure**

1. Navigate to **All** > **Policy and Compliance** > **Policy Exceptions** > **Exception Reason Choices**.
2. Click **New**.




3. On the form, fill in the fields.

**Reason Choice List form**

| Field | Description |
|---|---|
| Label | Enter a unique label for this choice. |
| Value | Enter a unique value for this choice. |
| Order | Enter an order for this choice. Reasons are ordered based on this number. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Default | Select this check box to indicate that this reason choice will be available whenever an ad hoc policy exception is requested. If the integration registry does not contain any application-specific choices, all reason choices with **Default** selected will be available. |
| Active | If this is selected, this choice is displayed in the list of reason choices. |

4. Click **Submit**.
   The reason choice is added and will be available in the **Reason** field of the policy exception request form for the selected application.
5. Repeat this process for as many reason choices as required by your users.

**Note:** For additional details about this process, see KB0783018.

### Define policy categories

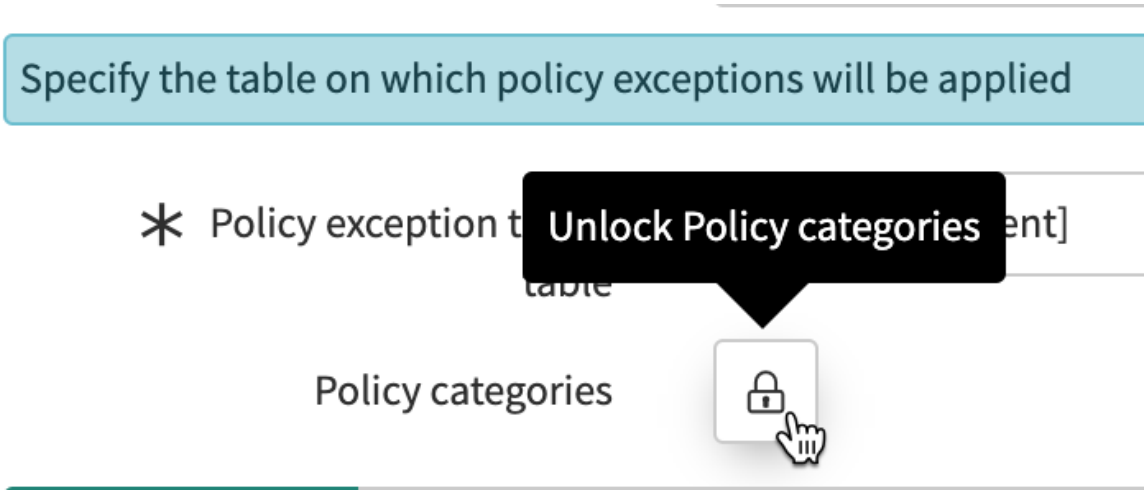
You can filter policies by specific criteria to limit the number of policies displayed when you are creating policy exceptions.

#### Before you begin

Role required: sn_compliance.manager

#### Procedure

1. When defining the Policy Exception Integration Registry, click the lock icon on the **Policy categories** field.




2. In the Policy categories form, click **New**.
3. Enter the name and description of the category you want to define.
4. Repeat for any other categories you want to define.
5. When you have finished defining categories, click the lock icon again.
   When you save the registry, the policy categories you defined are available on the Policy form for filtering policies.

#### Example:

Assume you defined registry entries for the Incident and Problem applications and selected Incident [incident] and Problem [problem] as the policy exception target tables. Also assume you created policy categories of **incident** and **problem**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You have defined five policies and they are tagged as follows.

- Policy 1 is tagged **incident**.
- Policy 2 is tagged **incident** and **VR**.
- Policy 3 is tagged **VR**.
- Policy 4 is tagged **Problem**.
- Policy 5 is untagged

You open the Problem form and click the **Request Policy Exception** button. You are prompted to enter specific details about the exception (for example, the policy, control objective, and so forth).

When you click the search icon in the **Policy** field, only Policy 1, Policy 2, and Policy 4 appear. If you select one of the three policies and click the search icon on the **Control objective** field, only control objectives related with that policy appear.

If none of your policies are tagged, all 5 appear. If you have only one policy tagged, that policy appears in the **Policy** field by default.

### Create an exception questionnaire

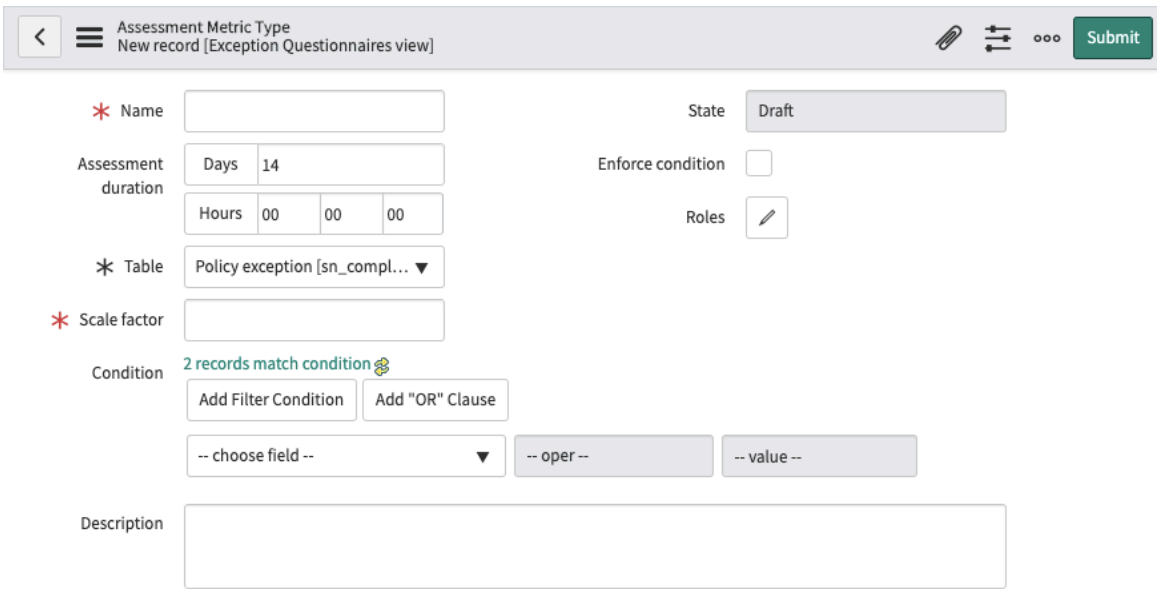
When you are setting up the Policy Exception Integration Registry, you can define configurable questions that can be included in risk assessments created from templates. The Policy Exception Integration Registry can be associated with one template at a time.

### Before you begin

Role required: sn_compliance.attestation_creator

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policy Exceptions** > **Exception Questionnaire**.
2. Click **New**.




**Note:** Notice that the Assessment Metric Type screen opened. In the terminology of GRC applications, a question in a questionnaire is considered a metric. A group of questions is a category. A group of categories is a metric type.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. On the form, fill in the fields.

**Assessment Metric Type form**

| Field | Description |
|---|---|
| Name | The name of the questionnaire. |
| Assessment duration | The amount of time allowed from the creation of the assessment to its completion. |
| Table | The table containing the records to be assessed. |
| Scale factor | The scale factor to be used for all questionnaire results. |
| State | The publish state of the assessment: **Draft** or **Published**. |
| Enforce condition | When selected, all records that do not meet the conditions defined are deleted. |
| Roles | Roles that have Read access to the information in the assessment. |
| Condition | Conditions for selecting records from the selected table to be assessed. For more information, see Condition builder. |
| Description | A description for this exception questionnaire. |

4. Save the questionnaire record.
5. Click **Attestation Designer** to create the questionnaire.
   For more information, see Attestation Designer.

### Define policy exception verification rules

The verification rule is used to verify the accuracy and completeness of a policy exception request prior to sending it out for approvals. You can define multiple levels of approvers for an application.

#### Before you begin

Role required:

- sn_compliance.manager to create the policy exception verification rules
- survey_reader to review and verify the questionnaire

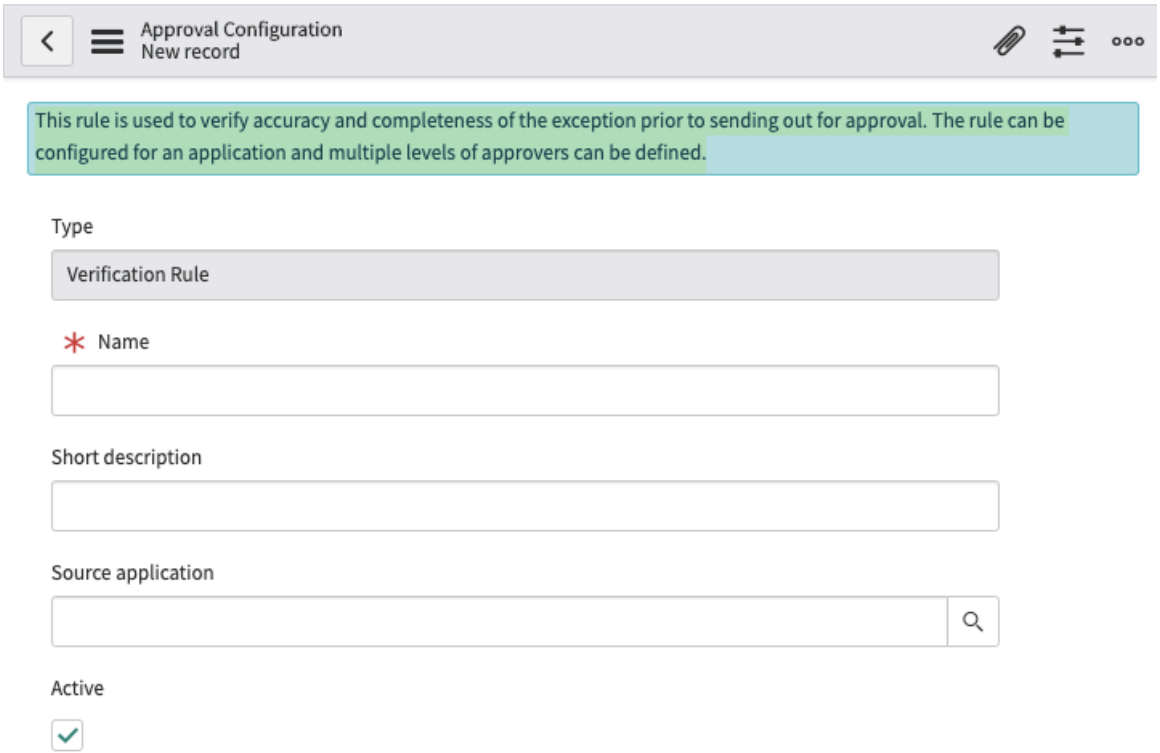
#### About this task

Defining verification rules is an optional step. If you do not define verification rules or define them and do not activate them, approvals from the requester's team will not be required.

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policy Exceptions** > **Verification Rule**.
2. Click **New**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. On the form, fill in the fields.

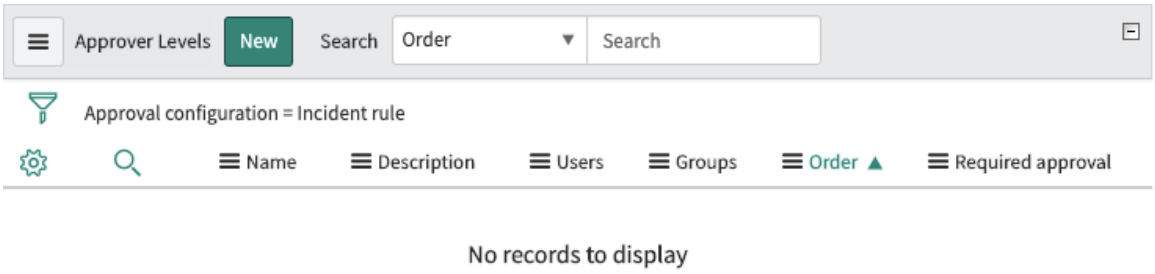
**Approval Configuration form**

| Field | Description |
|---|---|
| Type | Defaults to Verification Rule. |
| Name | Enter a name for this approval configuration. |
| Short description | Provide a brief description of the purpose of the configuration. |
| Source application | Select the application for that applies to this verification rule. Only applications that have been previously added to the Integration Registry are listed. |
| Active | If this is selected, this verification rule is active and the requester will have the option of requesting an initial approval prior to sending it to the compliance manager for approvals. |

4. Click **Update**.

The Approver Levels related list appears. This related list allows you to define multiple approver levels for a rule. One or more users, or a group of users can be selected as approvers for each level. Approvers must be assigned the survey_reader role. You can make it mandatory for all selected users to approve the exception or optionally allow a single user to approve on behalf of all approvers.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




5. Click **Submit**.
   When the policy exception record transitions to the Pending Verification state, the designated approvers are notified that their approval is required. If any fields in the policy exception request were not filled in by the requester (for example, the Policy or Control Objective), those fields become mandatory for the approvers. When the approvers have reviewed, completed, and approved the request, it transitions to the Analyze state and is assigned to the compliance manager for further analysis and approval.

### Define policy exception approval rules

Approval rules define the criteria (risk rating, policy or control objective) that is used for sending approval requests for an exception. Rules can be configured for an application and you can identify multiple levels of approvers, as needed.

#### Before you begin

Role required: sn_compliance.manager

#### About this task

You can configure approvals to be sent out automatically or manually after review.

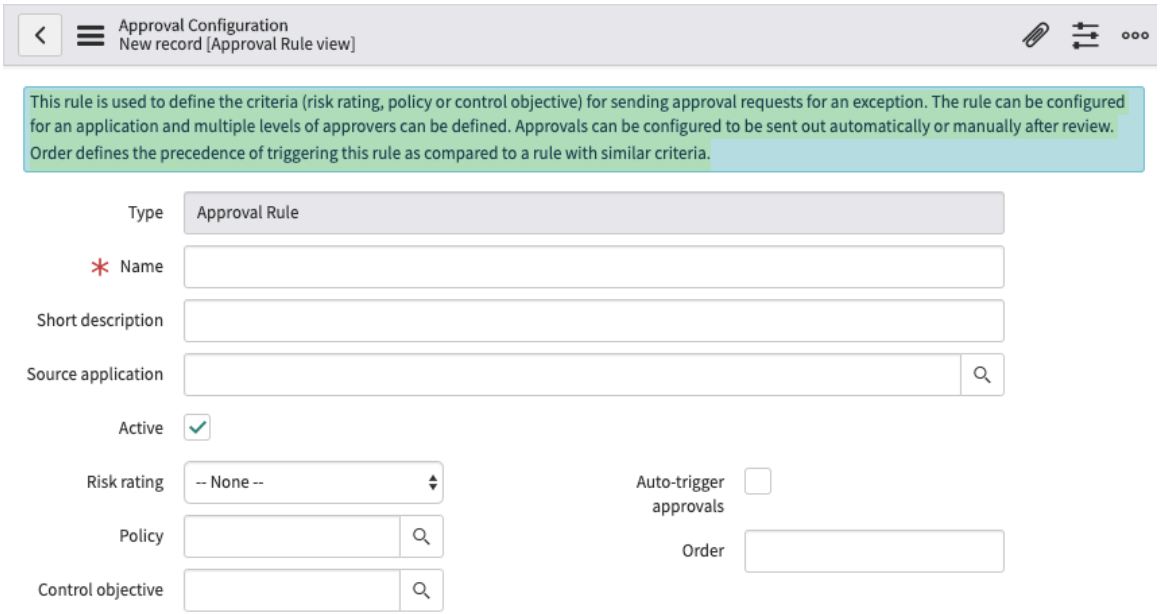
**Note:** When policy exceptions are created from upstream applications (from Vulnerability Response for example), the policy exception must have impacted controls present before you can request approval.

For policy exceptions created using Policy and Compliance Management, exceptions can be requested for a policy without impacted controls being present, even if both policies and control objectives are added to the exception form. However, for policy exceptions created for control objectives alone, impacted controls must be present before you can request approval.

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policy Exceptions** > **Approval Rule**.
2. Click **New**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. On the form, fill in the fields.

### Approval Configuration form

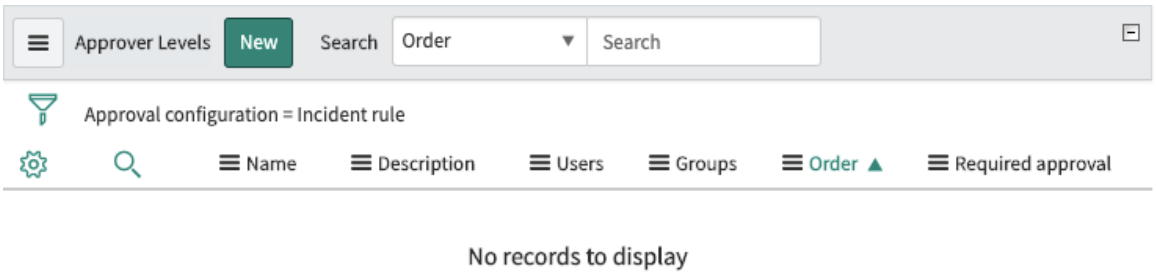
| Field | Description |
|---|---|
| Type | Defaults to Approval Rule. |
| Name | Enter a name for this approval configuration. |
| Short description | Provide a brief description of the purpose of the configuration. |
| Source application | Select the application for that applies to this approval rule. Only applications that have been previously added to the Integration Registry are listed. |
| Active | If this is selected, this approval rule is active. |
| Risk rating | The risk rating is determined by running a risk assessment on the policy exception. |
| Policy | Select the policy against which this policy exception is being applied. |
| Control objective | Select the control objective that references the selected policy. |
| Auto-trigger approvals | Select this check box to automatically trigger all approvals after the review is completed. If you do not select it, the compliance manager can manually trigger the approvals defined by this rule. |
| Order | Order defines the precedence of triggering this rule as compared to another rule that is applicable to the exception and defined with similar criteria. |

4. Click **Update**.

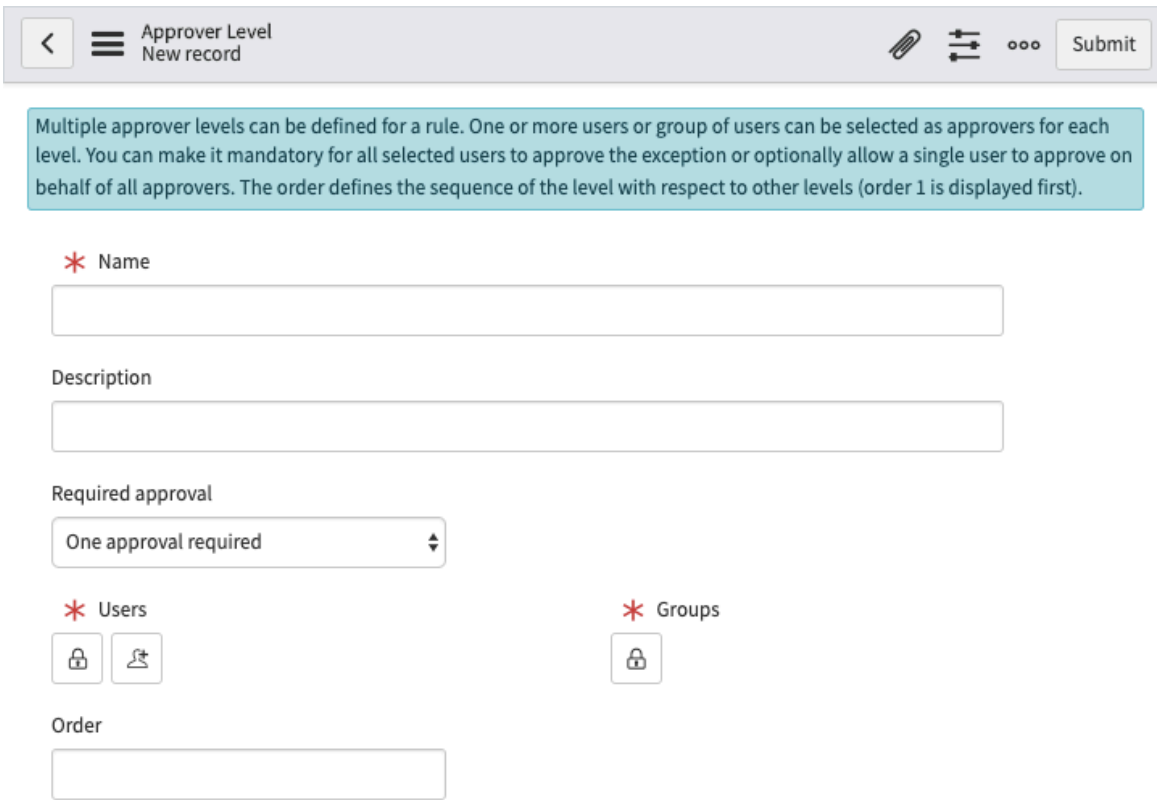
The Approver Levels related list appears. This related list allows you to define multiple approver levels for a rule. One or more users, or a group of users can be selected as approvers for each level. Approvers must be assigned the survey_reader role. You can

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

make it mandatory for all selected users to approve the exception or optionally allow a single user to approve on behalf of all approvers.




5. Click **New**.




6. On the form, fill in the fields.

### Approver Level form

| Field | Description |
|---|---|
| Name | Enter a name for this approval level. |
| Description | Provide a brief description of the approval level. |
| Required approval | Select **One approval required** to allow a single user to approve on behalf of all approvers.<br><br>Select **All users must approve** to make it mandatory that all designated users approve the selection. |
| Users | Select one or more users to act as policy exception approvers. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Groups | Select one or more groups to act as policy exception approvers.<br><br>**Note:** Users who belong to the group must have GRC business user (sn_grc.business_user) role. |
| Order | Select the order to determine the sequence of levels used with respect to other levels (that is, order 1 is displayed first). |

7. Click **Submit**.
   If you selected the **Auto-trigger approvals** check box, the designated approvers are notified that their approvals are required. Alternatively, the approvers are notified when the compliance manager clicks the **Send for Approval** button.

## Using the Classic user interface for Policy and Compliance tasks

You can continue to use the Classic environment to perform all Policy and Compliance Management activities.

As a compliance manager or compliance user with specific roles you can perform Policy and Compliance Management related tasks such as manage control objectives, policies, policy exceptions and extensions, issues, and others.

### Manage control objectives and policies

The Policies and Procedures module contains overview and detailed information related to policy approvals, policies, and control objectives.

### Policies and Procedures Overview

**Policies and Procedures Overview** is contained in the **Policies and procedures** module and provides an executive view into compliance requirements, overall compliance, and compliance breakdowns so areas of concern can be identified quickly. Users with the compliance administrator and compliance manager roles view the **Policies and Procedures Overview**.

#### Policies and Procedures Overview reports in the base system

| Name | Visual | Description |
|---|---|---|
| Control compliance | Donut chart | Displays the overall compliance of all the controls in the system. |
| Control details | Donut chart | Displays a breakdown of controls grouped by owner, category, or type. |
| Control Overview | Column Chart | Displays the total number of controls related to each policy. The chart is stacked to display the overall control compliance status for each policy. |
| Control Issues by Policy (Opened Date) | Line Chart | Displays the number of control issues opened each week, grouped by policy. |
| Policy Exceptions | List | Displays a list of control issues that have been closed with a response value of accept, meaning the issue was not remediated. |

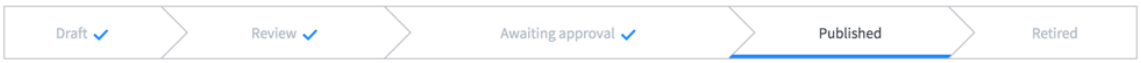
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Policies and Procedures Overview reports in the base system (continued)

| Name | Visual | Description |
|---|---|---|
| Total Control Objectives by Policy | Bar graph | Displays a count of the overall number of control objectives in each policy. The chart is stacked to display control objectives by type. |

## Policy approval process

Policies are part of a strict approval process that ensures compliance and reduces exposure to risk. When a policy is published, it is automatically incorporated in the approval process. Compliance managers set the length of time that policies are valid, ensuring that the team reviews the policy often to affirm its validity. Policies have a type, such as a policy, procedure, standard, plan, checklist, framework, or template.




### Policy approval states

| State | Description |
|---|---|
| Draft | All policies start in **Draft** state. In this stage, all compliance users can modify the policy and control objectives. |
| Review | The owner, owning group, and reviewers can modify the policy and control objectives and send it on to the next state. |
| Awaiting Approval | The policy is read only in this state. Approved policies transition to the **Published** state. Unapproved policies return to **Review**. If no approvers are identified on the policy form, the state is skipped and the policy is published without an approval. |
| Published | Approved policies are automatically published to a template-defined KB article, and the policy remains in a read-only state. The **Valid to** field on the policy form defines how long the policy is valid. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Policy approval states (continued)**

| State | Description |
|---|---|
| | **Note:** After the policy is published and when the valid to date on the policy is reached, then based on the value of the *Number of days after reaching a policy "Valid to" date in which the expired policy will automatically move from its Published state back to a Draft/Review state* property, the policy moves back to the Draft/Review state. For example, if the value of the property is 10, then the policy moves back to review state 10 days after the valid to date is reached.<br><br>When a policy reaches the end of the **Review** state and is **Approved** for publishing, it is automatically published to the GRC knowledge base (as defined in **Policy and Compliance** > **Administration** > **Properties**. The **Article template** field on the policy form defines the style of the published policy. |
| Retired | When a policy is put into the **Retired** state, its associated KB article is removed. |

## Policies

Compliance managers catalog and publish internal policies that define a set of business processes, procedures, and or standards.

## Control objectives

Compliance managers catalog the control objectives and generate controls from those control objectives.

**Note:** UCF refers to control objectives as controls. When UCF data is imported, controls are imported into the control objectives table.

### Create a policy

A policy defines an internal practice that processes must follow. Policies are defined as policies, procedures, standards, plans, checklists, frameworks, and templates.

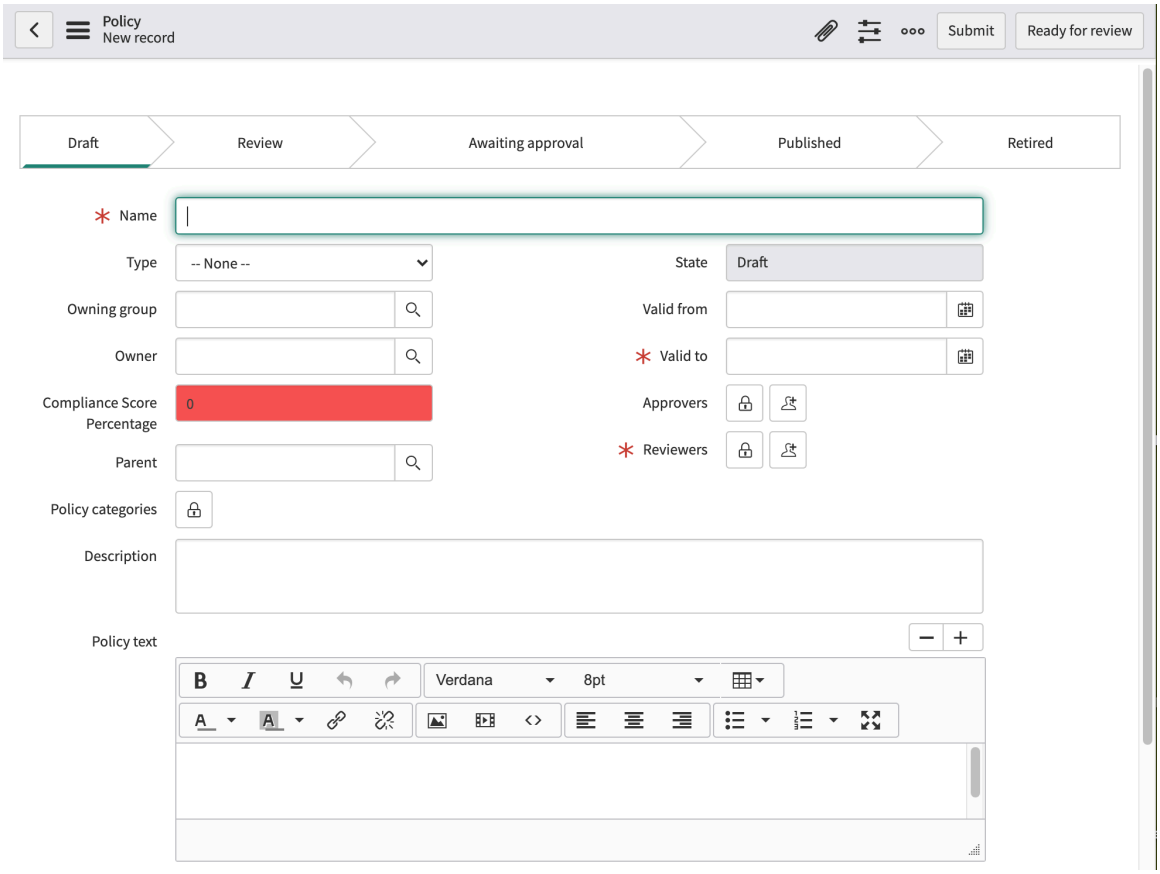
**Before you begin**
Role required: sn_compliance.admin or sn_compliance.manager

Users with Compliance user (sn_compliance.user) role can also create policies.

**Procedure**

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Policies**.
2. Click **New**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**3.** On the form, fill in the fields.

### Policy

| Field | Description |
|---|---|
| Name | The name of the policy. |
| Type | List of options:<br>◦ Policy<br>◦ Procedure<br>◦ Standard<br>◦ Plan<br>◦ Checklist<br>◦ Framework<br>◦ Template |
| Owning Group | Group that owns the policy. |
| Owner | User that owns the policy. |
| Compliance Score Percentage | The compliance score percentage assigned to this policy. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Parent | The policy containing this policy. If you create a control objective from within a policy, this field is automatically filled. |
| Policy categories | Click the lock icon and select one or more categories for filtering policies. For example, select Vulnerability Response to view policies associated with that application. |
| State | The state is a read-only field. Possible choices are:<br>◦ **Draft** In this state, all compliance users can modify the policy and control objectives. All compliance users can click **Request review** button. Enter a message in the Request review pop-up and click **Request** , which sets the state to Review.<br>◦ **Review** In this state, the owner, owning group, and reviewers can modify the policy and control objectives. The owner, owning group, and reviewers click **Request approval**, starting the workflow by sending approvals to the users in the Approvers list. The owner, owning group, and reviewers move the policy back to Draft, by clicking **Back to draft**, as well.<br>◦ **Awaiting approval** In this state, the policy and control objectives are read- only for all. Approvers can approve the policy by updating the approval state in the **Approvals** Related List on the policy form, or by viewing **My Approvals**. If the policy is approved, the policy goes to the **Published** state. Otherwise, it goes back to the **Review** state.<br>◦ **Published** In this state, the policy and control objectives are read-only for all. Admins can click **Retire** which sets the state of the policy to **Retired**<br>◦ **Retired** In this state, the policy is read-only for all. |
| Valid from | The date and time for which the policy becomes valid. |
| Valid to | The date and time for which the policy is no longer valid. |
| Approvers | The users you want to be included in the approval process. |
| Reviewers | Select the users you want to be included in the review process. |
| Description | A general description of the policy. |
| Policy text | A detailed description of the policy. |
| Knowledge Base | |
| Knowledge base | The knowledge base article related to this policy. |
| KB article | The KB article number and link where the policy is published. |
| Article template | The article template to use for the publication of this policy. |
| Acknowledgement Setup | |
| Audience | Select the default audience responsible for acknowledging this policy. |
| Reference Material URL | Click the lock icon to add the URL for any needed reference materials, such as certification or training materials. |
| Allow users to decline policy | Select this check box to give users the option of declining policy acknowledgements. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Allow users to request exception | Select this check box to give users the option of requesting exceptions for policy acknowledgements. |
| Exception Setup | |
| Maximum exception duration (days) | Enter the maximum number of days for which a policy exception can be requested for a given policy. |

4. Continue with one of the following options.
   - To save and submit the policy, click **Submit**.
   - To mark the policy ready for review, click **Request review** .

### What to do next
If you are implementing the Policy and Compliance Management software, return to the Policy and Compliance Management setup checklist and proceed to the next step.

## Approve and publish a policy

When a policy is approved, it is automatically published.

### Before you begin
Role required: sn_compliance_user or sn_compliance_manager

### About this task
Prior to Version 11.0.2 of the GRC: Policy and Compliance Management application, a new knowledge base article overwrote the previous version whenever you made changes to a policy. Starting with Version 11.0.2, when you again approve a policy, a new version of the KB article is created and listed in the **Policy Versions** tab, along with a history of previous versions.

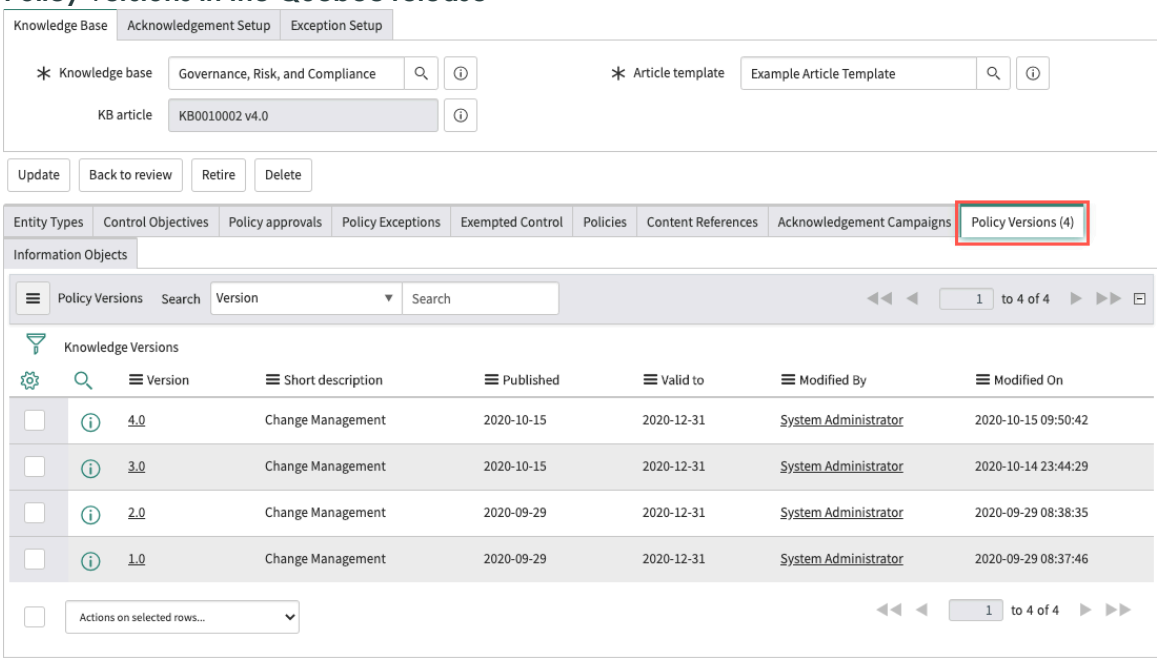
This feature requires that you manually install and activate the Knowledge Management Advanced Installer [com.snc.knowledge_advanced.installer] plugin. For more information, see Activate a plugin .

### Procedure
1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Policies**.
2. Open the policy record.
3. Review the policy details.
4. Click the **Request Approval** button.
   Reviewers cannot request approval for a policy. However, the owner of the policy and users with compliance manager role can request approval for a policy. When approval is granted, the policy is published and a knowledge base (KB) article is automatically created with the details of the policy.
5. Any time you need to make changes to the policy, you can click **Edit policy** and enter a message in the pop-up, and click **Request Approval**. Add a comment in the pop-up. When approval is granted, a new version of the knowledge base article is created.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** As described above, if you activated the Knowledge Management Advanced Installer [com.snc.knowledge_advanced.installer] plugin, a new version of the KB article is created and listed in the **Policy Versions** tab, along with a history of previous versions as shown below.

**Policy versions in the Quebec release**




So, if you create links to this policy from the Service Portal or elsewhere, the latest version of the KB article is always displayed.

### Acknowledge a policy

After a policy has been published, you can create an acknowledgement campaign to define a group of your employees who must provide an acknowledgement that a particular policy is in compliance. When the campaign has been defined, you can submit the request to the audience.

### Set up a policy acknowledgement campaign

A policy campaign is the record used to prepare for a policy acknowledgement request. It defines the audience who must provide an acknowledgement that a particular policy is in compliance. A policy campaign is requested only if the compliance user decides it is needed.

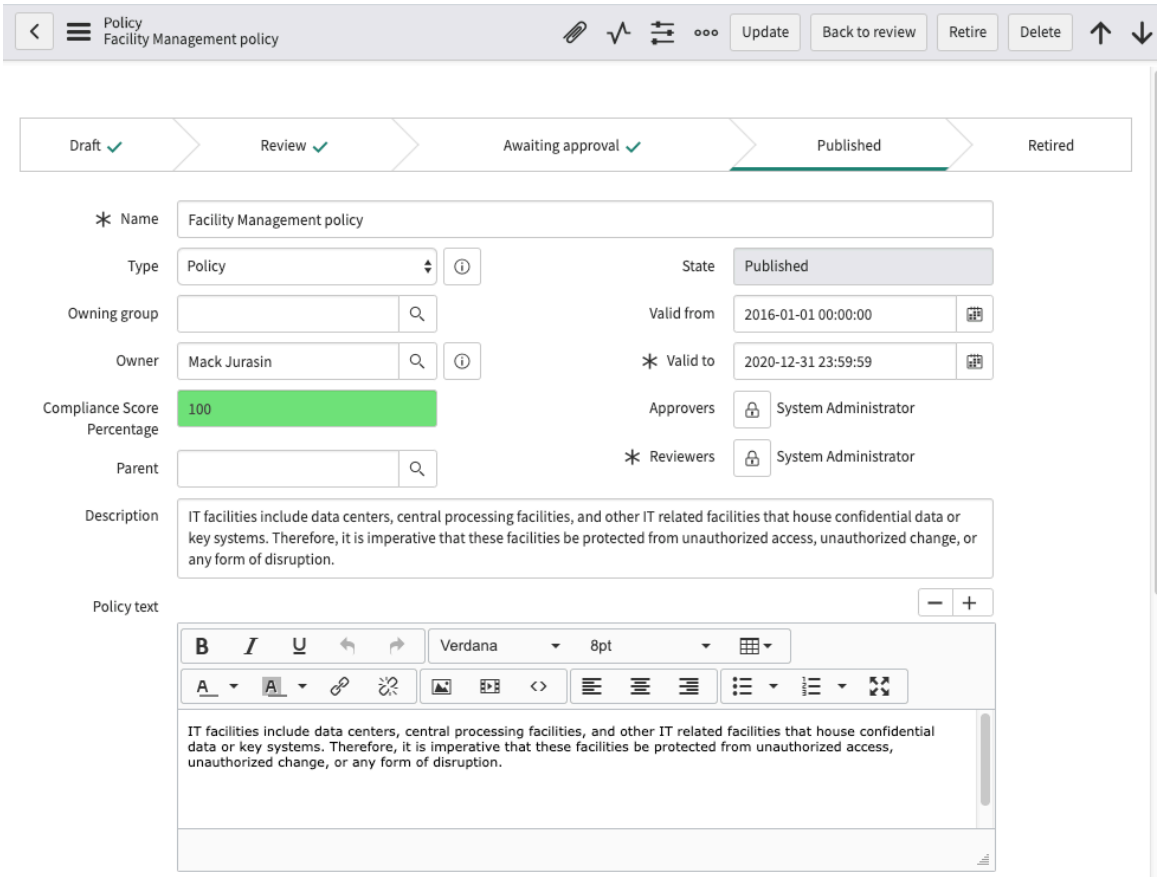
#### Before you begin

Role required: Compliance User

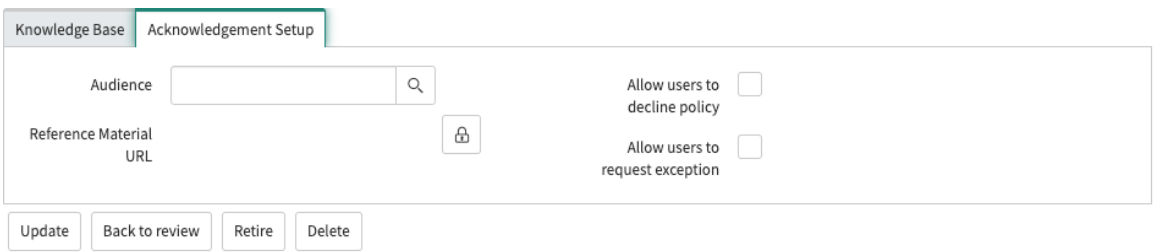
#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Policies**.
2. Open the Policy record in the **Published** state you want to acknowledge.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**3.** Scroll down and click the **Acknowledgement Setup** related list.



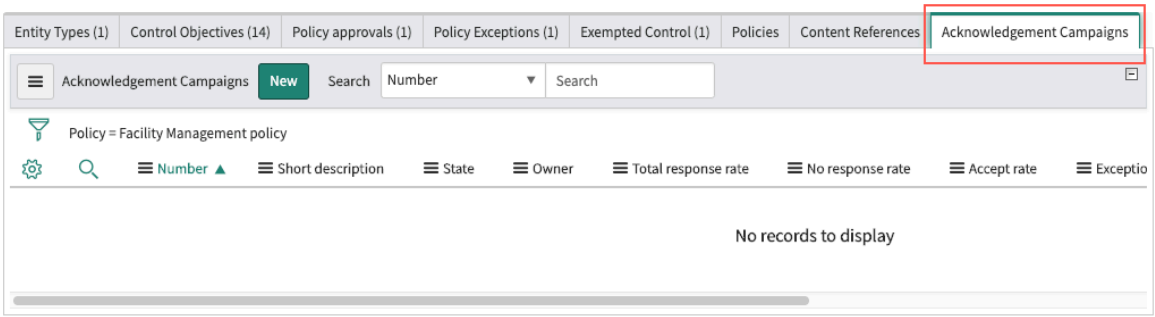

**4.** On the form, fill in the fields.

| Field | Description |
|---|---|
| Audience | Select the employees who are responsible for acknowledging the policy. You define the audience using the Audience module. |
| Reference Material URL | Click the lock icon and add a URL to reference materials for the policy that the audience can review. When you have completed your entry, click the lock icon again. |
| Allow users to decline policy | Select if you want members of the audience to be able to decline the policy. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

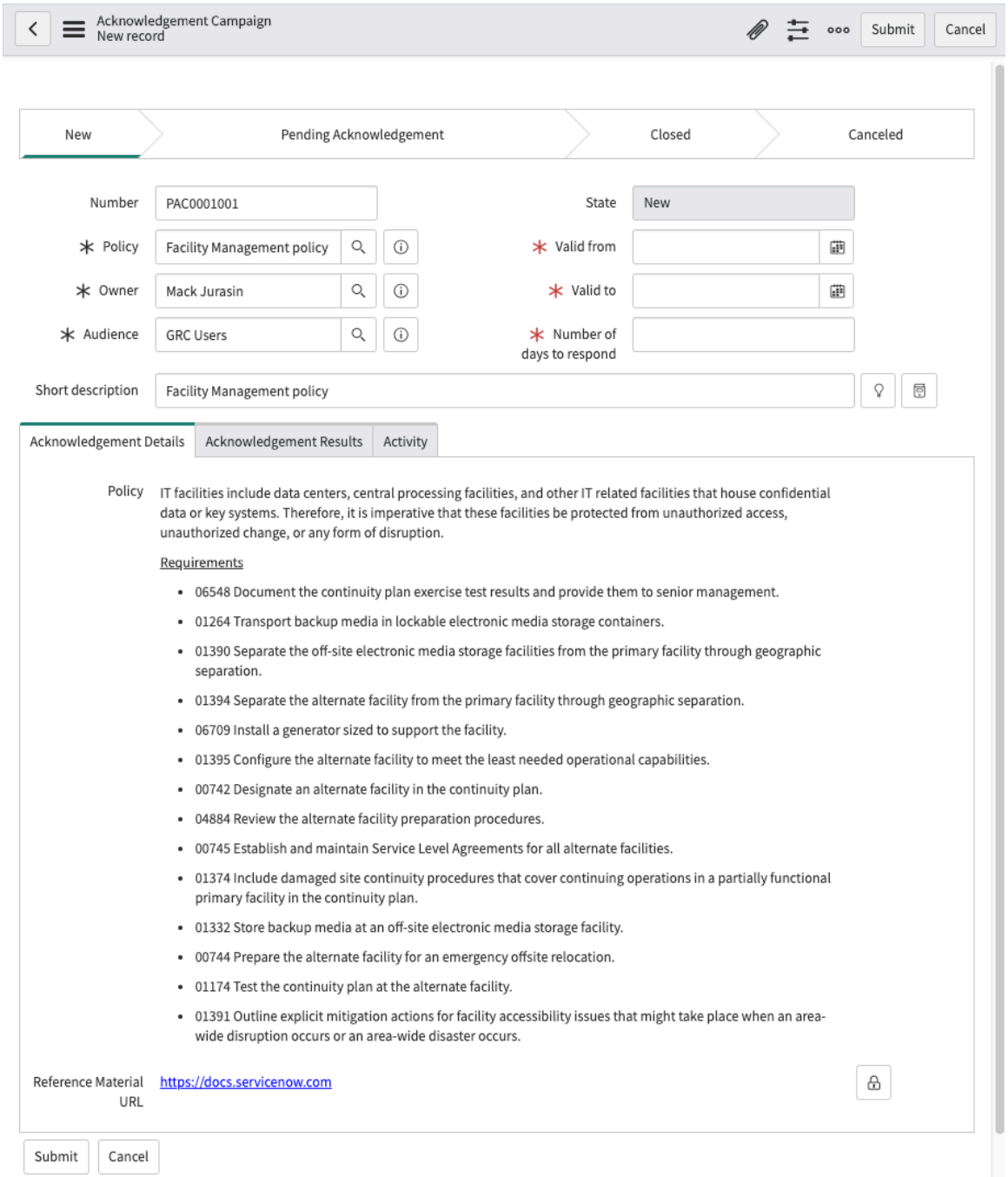
| Field | Description |
| --- | --- |
| Allow users to request exception | Select if you want to members of the audience to be able to request a policy exception. |

5. Save the record.
6. Scroll down and click the **Acknowledgement Campaigns** related list.




7. Click **New**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**Note:** Notice that the majority of the fields are pre-filled with data from the policy record.

8. On the form, fill in the fields.

**Note:** Only field description that were not previously described are provided here.

| Field | Description |
|---|---|
| Number | An auto-generated record number for the acknowledgement. |
| State | The current state of the acknowledgement campaign. The default state is New. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Valid from/to | Select the period of time the acknowledgement is valid. The acknowledgement is valid from the beginning of the **Valid from** date until the end of the **Valid to** date.<br><br>**Note:** The **Valid from** date cannot be prior to the current date. The **Valid to** date cannot be beyond the **Valid to** date defined in the policy. |
| Number of days to respond | The number of days by which members of the audience have to respond. |
| Short description | A brief description of the policy. |
| **Acknowledgement Details** tab | This tab shows details and requirements from the policy, as well as the **Reference Material URL** defined during acknowledgement setup. |

9. Click **Submit**.
   The acknowledgement request is now ready for you to send to the defined audience.

### Create an audience

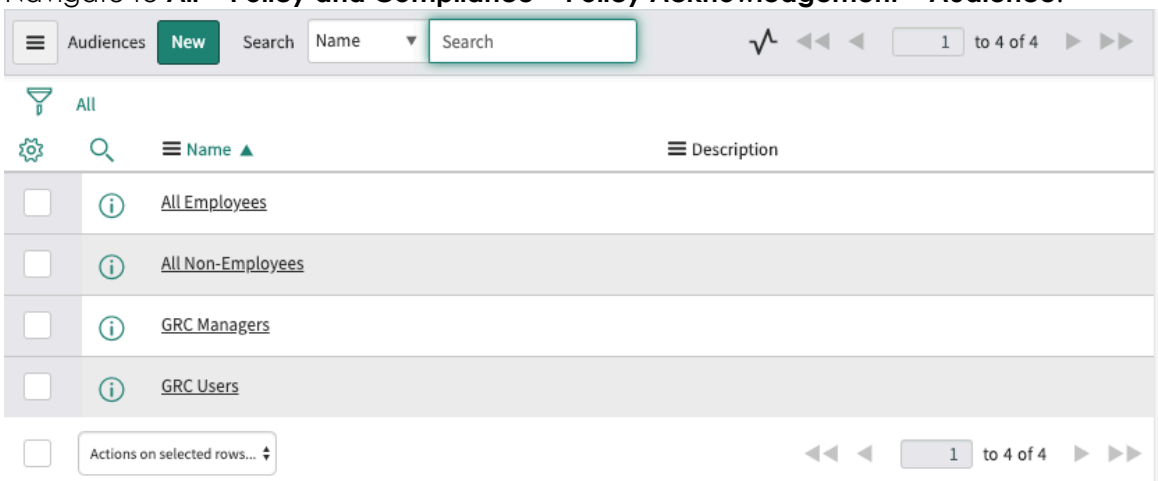
When you set up a policy acknowledgement request, you must identify an audience responsible for providing the acknowledgement.

#### Before you begin

Role required: sn_compliance_admin or sn_compliance_manager

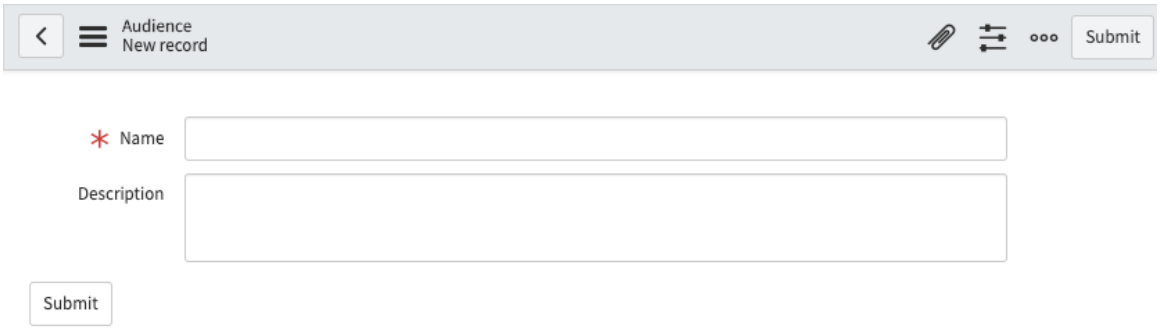
#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policy Acknowledgement** > **Audience**.

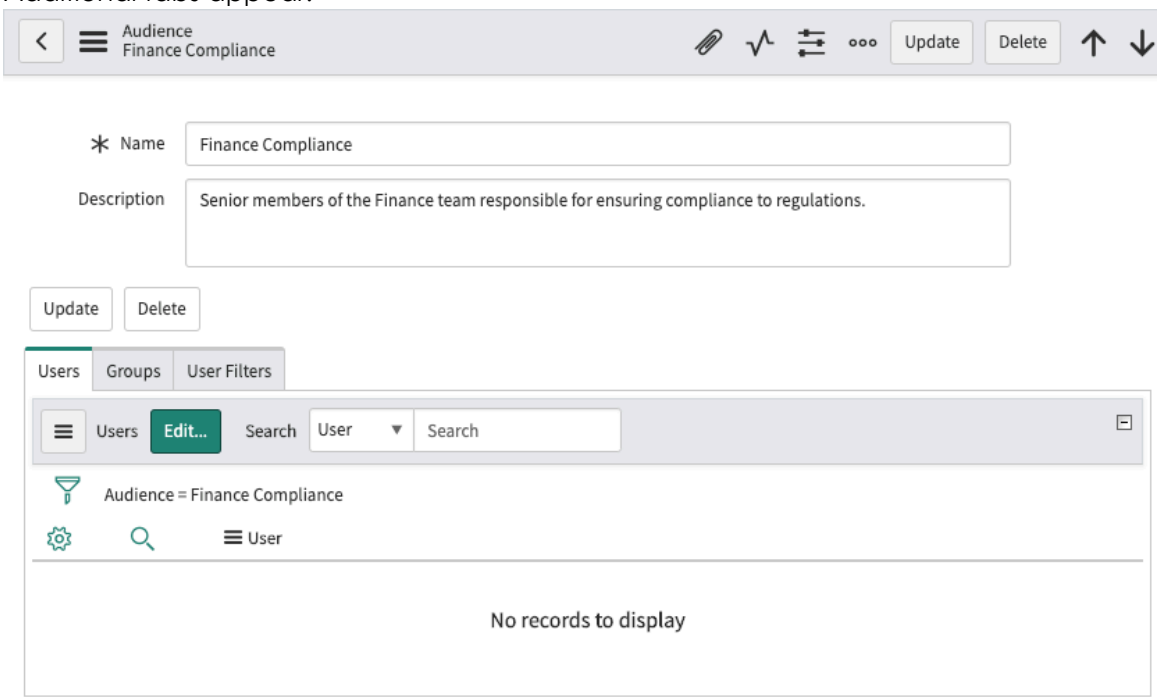



2. Click **New**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. Enter a name and description for the new audience, and save the record.
4. Additional tabs appear.




5. Use the three tabs to identify members for this audience.

| Option | Description |
|---|---|
| Users | Click **Edit** and add one or more individual users to the audience. |
| Groups | Click **Edit** and add one or more predefined groups of users to the audience. |
| User Filters | Click **New** to define a new filter for audience member inclusion. Click **Edit** to modify an existing user filter. You can save filters for future use. |

6. When the audience has been defined, you can add the users, groups, or user filters to anacknowledgement request.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Submit an acknowledgement request

After you have created an acknowledgement campaign, you can submit the acknowledgement request to the defined audience.

**Before you begin**
Role required: sn_compliance.user

**Procedure**

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **My Acknowledgement Campaigns**.
2. Open the Policy Acknowledgement Campaign (PAC) record you want to submit to the defined audience.
3. Ensure that you have set up and saved the acknowledgement in the Acknowledgement Setup related list.
4. Click the **Acknowledgement Campaigns** related list.
5. Click **New**.

   **Note:** The majority of the fields are pre-filled with data from the policy record.

6. On the form, fill in the fields.

   **Note:** Only field description that were not previously described are provided here.

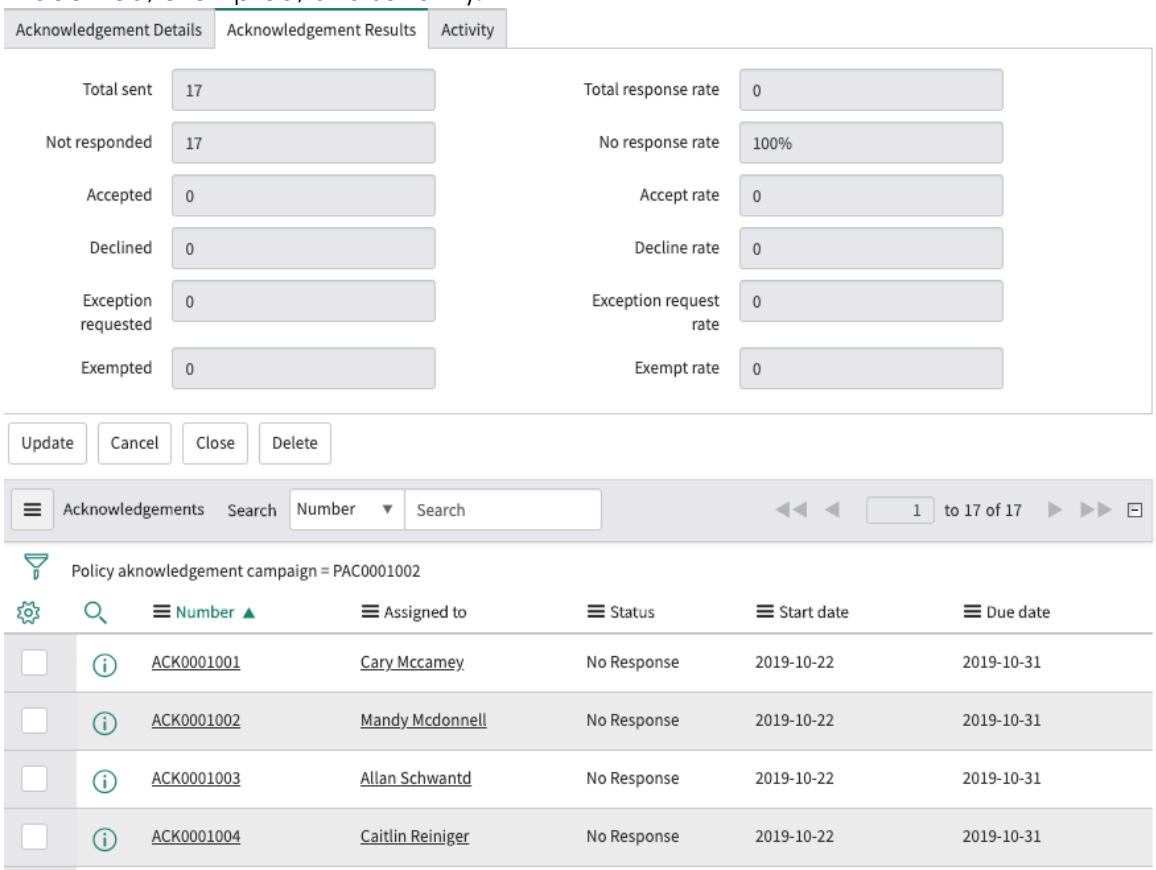
   **Acknowledgement Campaign form**

| Field | Description |
|---|---|
| Number | An auto-generated record number for the acknowledgement. |
| State | |
| Valid from/to | Select the period of time the acknowledgement is valid. The acknowledgement is valid from the beginning of the **Valid from** date until the end of the **Valid to** date.<br>**Note:** The **Valid to** date cannot be beyond the **Valid to** date defined in the policy. |
| Number of days to respond | The number of days by which members of the audience have to respond. |
| Short description | A brief description of the policy. |
| **Acknowledgement Details** tab | This tab shows details and requirements from the policy, as well as the **Reference Material URL** defined during acknowledgement setup. |

7. Click **Submit**.
   The **Request Acknowledgement** button appears.
8. Click **Request Acknowledgement**.
9. Notice that the following changes occur.
   - The state of the acknowledgement campaign changes to **Pending Acknowledgement**.
   - Acknowledgement (ACK) records for each member of the audience appear at the bottom of the screen.

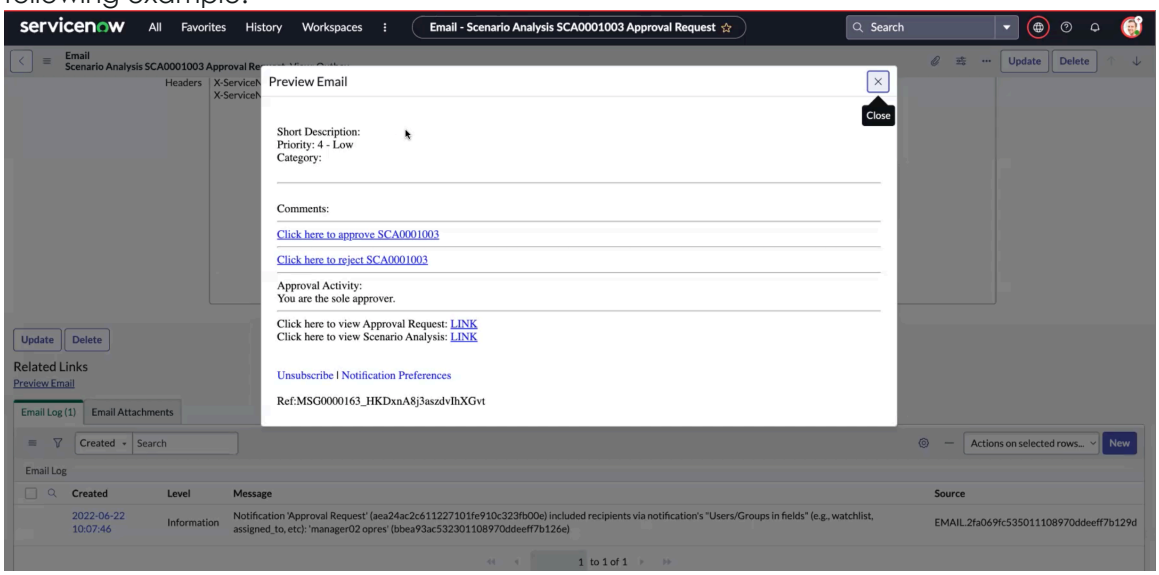
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The **Acknowledgement Results** tab shows the progress of the acknowledgement process. That is, it reports the total number of acknowledgements sent, and keeps a running tally of the number and types of responses received (for example, number of accepted, declined, exempted, and so forth).




**Note:** The **Activity** tab shows acknowledgement activities as they happen. The compliance user can click the Work notes check box and post work notes to track changes. The Additional comments box can be used to communicate with the audience.

Also, each member of the audience receives an email notification similar to the following example.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. As the acknowledgement period elapses, you can monitor the progress of the responses by navigating to **Policy and Compliance** > **Policy Acknowledgement** > **Pending Acknowledgements**.
11. You can also identify any audience members who have exceeded the acknowledgement time line by navigating to **Policy and Compliance** > **Policy Acknowledgement** > **Overdue Acknowledgements**.

### Respond to an acknowledgement request

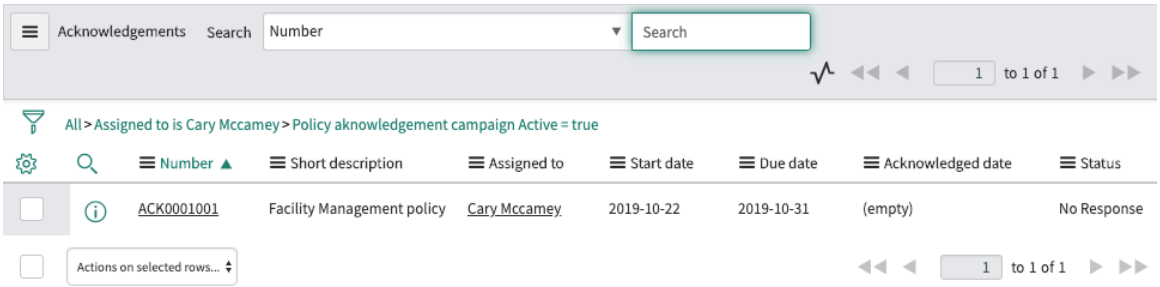
After you have been identified as a member of an audience to provide a policy acknowledgement, you must open and review the record, and then acknowledge it.

#### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

#### Procedure

1. After you have received a notification that you are required to acknowledge a policy, navigate to **Policy and Compliance** > **Policy Acknowledgement** > **My Acknowledgements**.




2. To provide the acknowledgement, open the record and perform one of the following actions.

   The available options depend on how the acknowledgement request was configured.

   - If the policy is in compliance, click **Accept**.
   - If the policy is not in compliance and the request is configured in such a way that you are allowed to decline the request, click **Decline**.
   - If, for any reason, you do not want to respond, and the request is configured in such a way that you can opt out, click **Request Exception**.

### Work with acknowledgements using the service portal

After you have received a request to provide acknowledgement for a policy, you have the option of working with the request in the Now Platform, or you can perform your actions in the ServiceNow Service Portal.

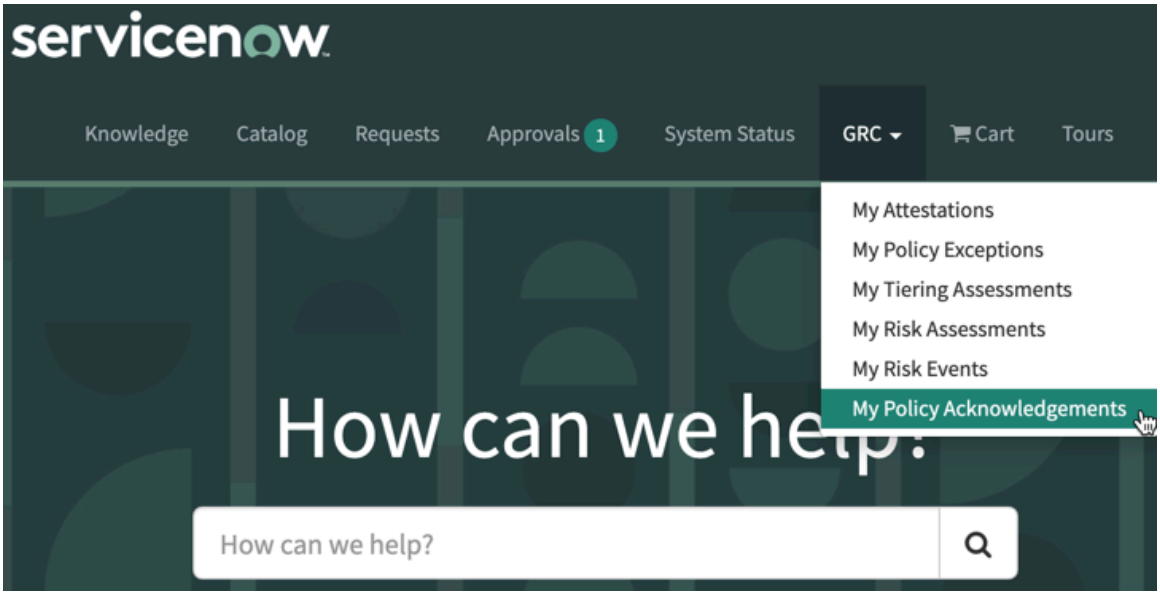
#### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

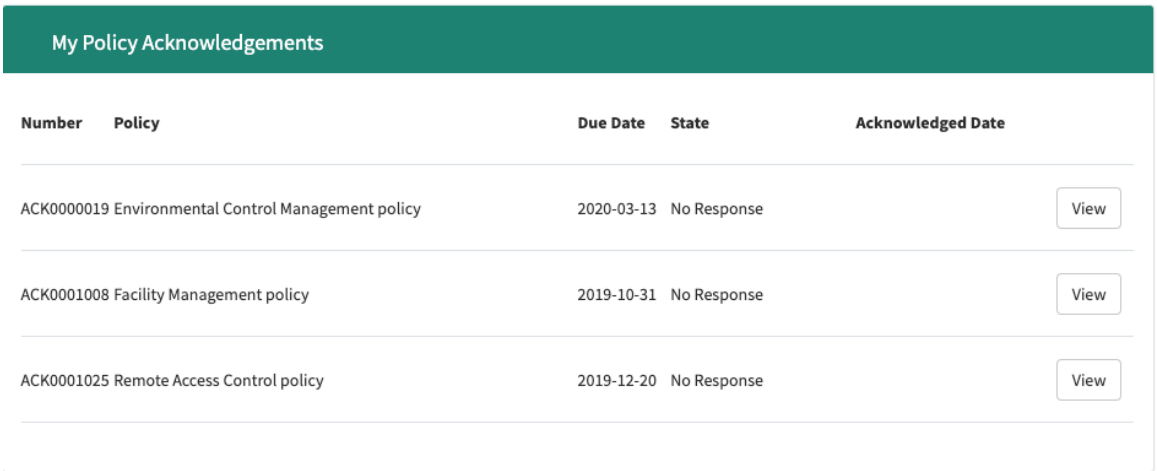
#### Procedure

1. Navigate to the ServiceNow Service Portal.
2. In the header bar, navigate to **GRC** > **My Policy Acknowledgements**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

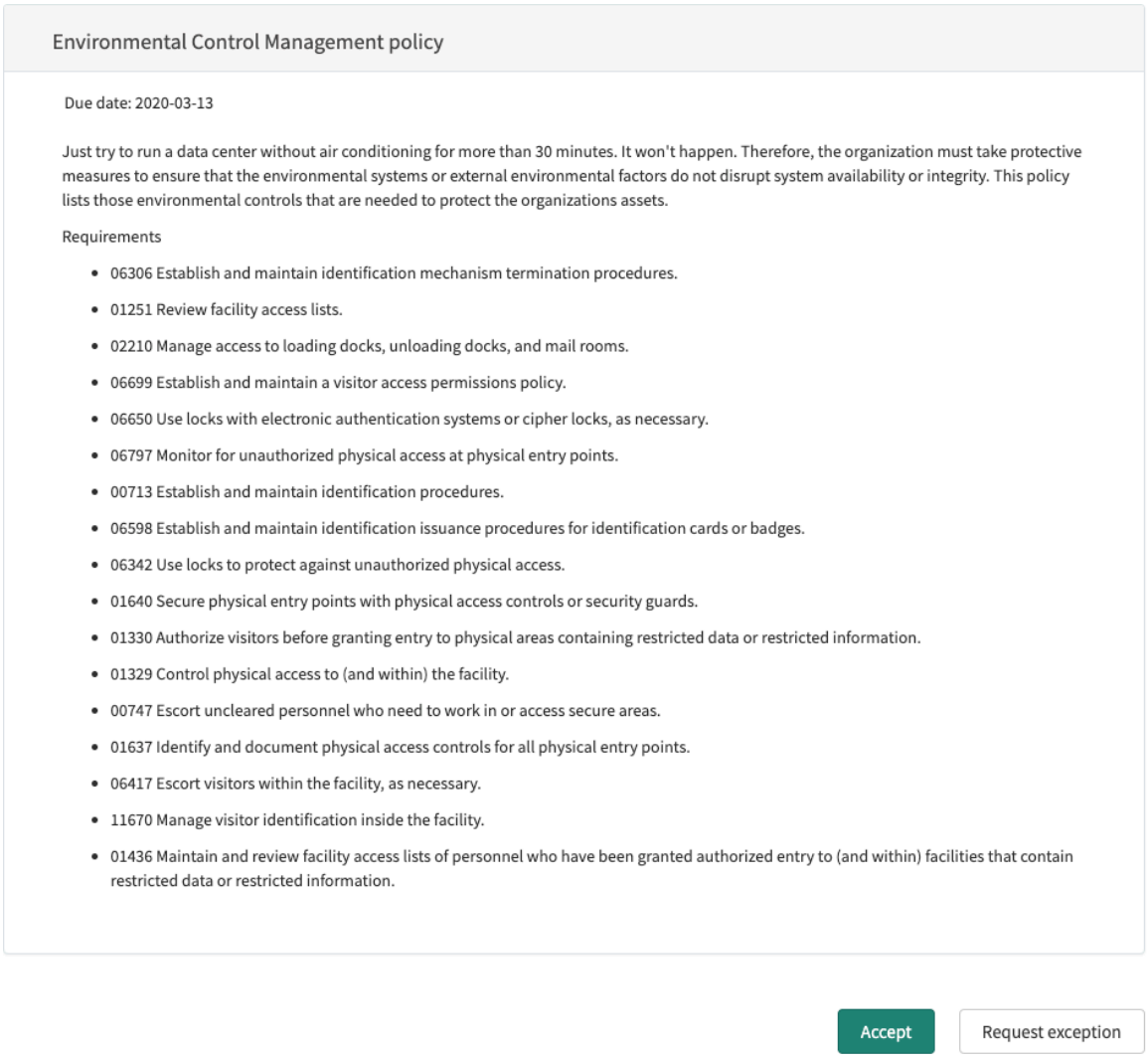



All pending policy acknowledgement requests assigned to you appear.




**3.** To view details of the request, click **View**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**Note:** The actions you can perform on the policy acknowledgement depend on how the acknowledgement campaign was configured, as follows.

| Option | Description |
|---|---|
| If the policy is in compliance | Click **Accept**. |
| If the policy is not in compliance and you are allowed to decline the request | Click **Decline**. |
| If you do not want to respond, and you want to opt out | Click **Request Exception**. |

### Retire a policy

Retiring a policy is part of the policy management process. It can be retired anytime after being approved and published to the KB.

**Before you begin**
Role required: sn_compliance_admin or sn_compliance_manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policies**.
2. Open the Policy record.
3. In the top-right corner, click **Retire**.
   This option is available only for policies in a published state.

## Create a GRC article template

Policy and Compliance managers can create templates for policy article publishing.

### Before you begin

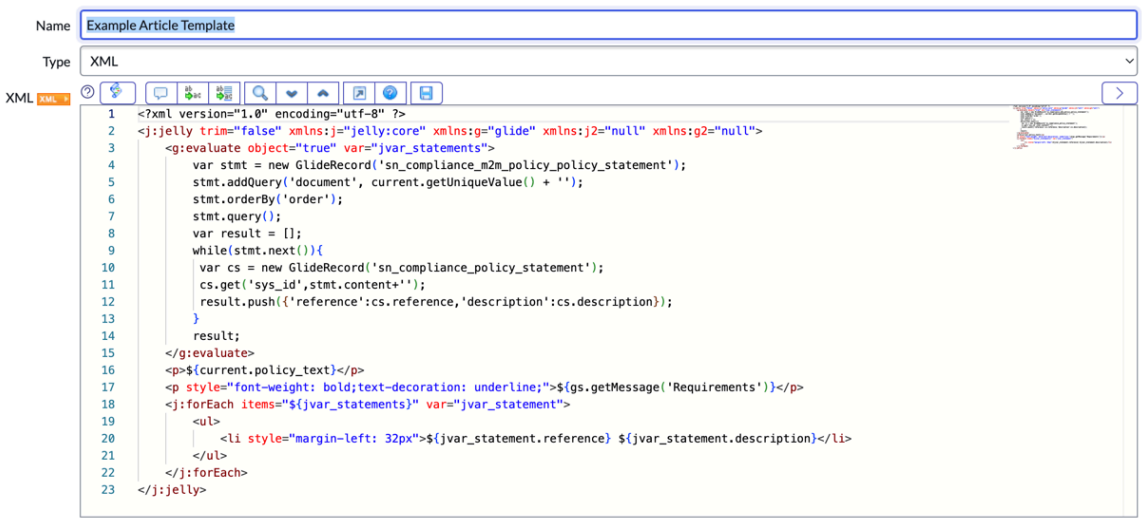
Role required: sn_compliance.developer

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Article Templates**.
2. Click **New**.
3. On the form, fill in the fields.

#### Authority Document

| Field | Description |
|---|---|
| Name | Name of the article template. |
| Type | ◦ Script<br>◦ HTML<br>◦ XML |
| Script | The script code. This field depends on the **Type** field. |
| HTML | The HTML code. This field depends on the **Type** field. |
| XML | The XML code. This field depends the **Type** field. |
| Is default | Option to indicate that this template is used as the default template for all KB articles. |




4. Click **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create a control objective

A control objective is an objective, direction, or standard that acts as guidance for company interactions and operations. Control objectives can be categorized, classified, and related to policies.

## Before you begin

Role required: sn_compliance.admin, sn_compliance.manager, sn_compliance.user

## Procedure

1. Navigate to **All** > **Policy and Compliance** > **Control Objectives**.
2. Click **New**.
3. On the form, fill in the fields.

### Control Objectives form

| Field | Description |
|---|---|
| Name | Name of the control objective. |
| Source | Source of the control objective. For example, if the control objective is from a third-party provider, indicate which one. |
| Source ID | Unique identification number used by the source to catalog this control objective. |
| Reference | Unique numerical identifier. |
| Parent | Control objective that is not a child of the current control objective. This is to avoid cyclic parent – child relationship. |
| Compliance Score Percentage | Compliance score percentage calculated for this control objective and it's color code:<br>◦ 80 and higher in green<br>◦ 80 to 50 in yellow<br>◦ below 50 in red |
| Active | Option that indicates whether a control objective is active. |
| Creates controls automatically | Option that indicates that controls are automatically created from the control objective.<br>**Note:** Select this option if the control objective can also serve as the control. |
| Category | List of options:<br>◦ Acquisition or sale of facilities, technology, and services<br>◦ Audits and risk management<br>◦ Compliance and Governance Manual of Style<br>◦ Human Resources management<br>◦ Leadership and high-level objectives<br>◦ Monitoring and measurement<br>◦ Operational management |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Physical and environmental protection<br>◦ Privacy protection for information and data<br>◦ Records management<br>◦ System hardening through configuration management<br>◦ Systems continuity<br>◦ Systems design, build, and implementation<br>◦ Technical security<br>◦ Third Party and supply chain oversight<br>◦ Root<br>◦ Deprecated |
| Classification | List of options:<br><br>◦ Preventive<br>◦ Corrective<br>◦ Detective |
| Type | List of options:<br><br>◦ Acquisition/Sale of Assets or Services<br>◦ Actionable Reports or Measurements<br>◦ Audits and Risk Management<br>◦ Behavior<br>◦ Business Processes<br>◦ Communicate<br>◦ Configuration<br>◦ Data and Information Management<br>◦ Duplicate<br>◦ Establish Roles<br>◦ Establish/Maintain Documentation<br>◦ Human Resources Management<br>◦ Investigate<br>◦ IT Impact Zone<br>◦ Log Management<br>◦ Maintenance<br>◦ Monitor and Evaluate Occurrences<br>◦ Physical and Environmental Protection<br>◦ Process or Activity<br>◦ Records Management<br>◦ Systems Continuity |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ Systems Design, Build, and Implementation<br>◦ Technical Security<br>◦ Testing<br>◦ Training |
| Attestation | List of options.<br>◦ **GRC Attestation** is chosen by default<br>◦ **Note:** If the user changes the control attestation, the related control objective attestation type is changed also. |
| Issue group rule | Group rule assigned to this control objective. |
| Description | Description of the control objective. |

4. Click **Submit**.
   The control objective is created and all related lists are visible.
   - A control is created for every control objective when a policy is associated with an entity.
   - The control attributes default to the same attributes as the related control objective.

### What to do next
If you are implementing the Policy and Compliance Management software, return to the Policy and Compliance Management setup checklist and proceed to the next step.

#### Deactivate a control objective

Deactivate control objectives that are no longer relevant to their citation or parent control objective.

### Before you begin
Role required: sn_compliance_admin or sn_compliance_manager

### Procedure
1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Control objective**.
2. Open a control objective.
3. In the control objective, clear the check box marked **Active**.
4. Click **Update**.

#### Relate a control objective to a policy

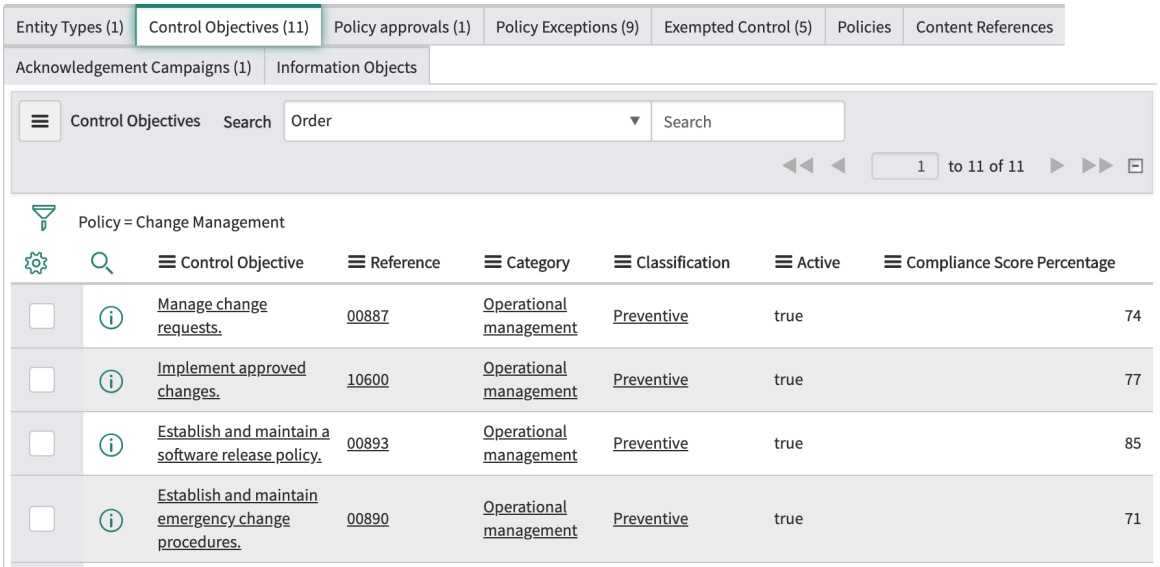
Associate the control objective to a policy individually when the policy is in the review or draft state by clicking the edit button in the Control Objective related list.

### Before you begin
Role required: sn_compliance.admin, sn_compliance.manager, sn_compliance.user

### Procedure
1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Policies**.
2. Open the policy record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click **Edit** in the **Control Objectives** related list.
   The slushbucket contains active control objectives with no associated policy selected.
4. Select the control objectives.
5. Click **Save**.
   Those control objective are listed in the **Control Objective** related list.




## What to do next

If you are implementing the Policy and Compliance Management software, return to the Policy and Compliance Management setup checklist and proceed to the next step.

### Relate a control objective to a citation

A single control objective can be mapped to many citations from different authority documents. This function allows you to test a control objective once while complying with many different citations.

## Before you begin

Role required: sn_compliance_admin or sn_compliance_manager

## Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance** > **Citations**.
2. Open a citation.
3. In the **Control Objectives** related list, click **New**.
4. On the form, fill in the fields.

### Control objective form

| Field | Description |
|---|---|
| Name | Name of the control objective. |
| Source | Source of the policy. For example, if the statement is from a third-party provider, indicate which one. |
| Source ID | Unique identification number used by the source to catalog this authority document. |
| Reference | Unique numerical identifier. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Policy | Parent control objective supported by this control objective. |
| Parent | References the parent content. |
| Active | Option that indicates if a policy is active. If the control objective is not in the **Draft** or **Retired** states, a policy is marked active. |
| Category | Select from a list of options:<br><br>◦ Acquisition or sale of facilities, technology, and services<br>◦ Audits and risk management<br>◦ Compliance and Governance Manual of Style<br>◦ Human Resources management<br>◦ Leadership and high-level objectives<br>◦ Monitoring and measurement<br>◦ Operational management<br>◦ Physical and environmental protection<br>◦ Privacy protection for information and data<br>◦ Records management<br>◦ System hardening through configuration management<br>◦ Systems continuity<br>◦ Systems design, build, and implementation<br>◦ Technical security<br>◦ Third Party and supply chain oversight<br>◦ Root<br>◦ Deprecated |
| Classification | Select from a list of options:<br><br>◦ Preventive<br>◦ Corrective<br>◦ Detective<br>◦ IT Impact Zone |
| Type | Select from a list of options:<br><br>◦ Acquisition/Sale of Assets or Services<br>◦ Actionable Reports or Measurements<br>◦ Audits and Risk Management<br>◦ Behavior<br>◦ Business Processes<br>◦ Communicate<br>◦ Configuration<br>◦ Data and Information Management |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ Duplicate<br>◦ Establish Roles<br>◦ Establish/Maintain Documentation<br>◦ Human Resources Management<br>◦ Investigate<br>◦ IT Impact Zone<br>◦ Log Management<br>◦ Maintenance<br>◦ Monitor and Evaluate Occurrences<br>◦ Physical and Environmental Protection<br>◦ Process or Activity<br>◦ Records Management<br>◦ Systems Continuity<br>◦ Systems Design, Build, and Implementation<br>◦ Technical Security<br>◦ Testing<br>◦ Training |
| Description | Description of the control objective and how it supports the goals of the organization. |

5. Click **Submit**.
   The control objective that you created is related to the citation.

### Create or deactivate a citation

Usually, authority documents, citations, and control objectives are downloaded from a third-party provider. However, citations can be created manually from an authority document. The **Active** option in a citation indicates whether the citation is active or inactive.

## Before you begin

Role required: sn_compliance_admin or sn_compliance_manager

## Procedure

1. Navigate to **All** > **Policy and Compliance** > **Authority Documents**.
2. Open an authority document.
3. In the **Citations** related list, click **New**.
4. On the form, fill in the fields.

### Citation form

| Field | Description |
|---|---|
| Name | User-defined name that identifies this citation. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Source | Source of the policy. For example, if the statement is from a third-party provider, indicate which one. |
| Source ID | Unique identification number used by the source to catalog this authority document. |
| Reference | Content reference. |
| Type | Type of citation created. Optional field not used for any processing. Use the value in this field in reports or to query for records of a specific type.<br>◦ Core Topic<br>◦ Process<br>◦ Control Objective<br>◦ Control<br>◦ Supporting information |
| Authority document | Name of the parent authority document for this citation. When you create citations from the authority document form, the system completes this field automatically. |
| Active | Option that indicates if a policy is active. A policy is marked active if it is not in the **Draft** or **Retired** state. To deactivate a citation, clear the check box marked **Active**. |
| Parent | References the parent content. |
| Description | Description of the citation. |

5. In the Settings related list, select the **Functional domain** field.
6. Select a domain.
   Only the citations specific to the selected domain appear in your application.

### Create an authority document

Authority documents manage a process and citations are created within them to manage points of the process. For example, the process called Building Security contains a citation for Entry Control.

#### Before you begin

Role required: sn_compliance_admin or sn_compliance_manager

#### Procedure

1. Navigate to **Policy and Compliance** > **Compliance** > **Authority Documents**.
2. Click **New**.
3. On the form, fill in the fields.

#### Authority Document

| Field | Value |
|---|---|
| Name | Name of the document. |
| Number | Read-only field that is automatically populated with a unique identification number. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Value |
|---|---|
| Source | A non-editable field with the source of the policy. For example, if the statement is from the UCF import, the source is UCF. |
| Source ID | The unique identification number used by the source to catalog this authority document. |
| Version | The unique version number used by the source to identify this authority document. |
| Common name | Abbreviated version of the **Name** field. |
| Category | Category for this authority document. |
| Type | The document type:<br>◦ Audit Guideline<br>◦ Best Practice Guideline<br>◦ Bill or Act<br>◦ Contractual Obligation<br>◦ International or National Standard<br>◦ Not Set<br>◦ Organizational Directive<br>◦ Regulation of Statute<br>◦ Safe Harbor<br>◦ Self-Regulatory Body Requirement<br>◦ Vendor Documentation |
| Valid From | The date and time for which the policy becomes valid. |
| Valid To | The date and time for which the policy is no longer valid. |
| Url | The URL of the stored authority document. |
| Description | More information about the authority document. |

4. Right-click in the header bar and select *Save* from the context menu.
   The authority document is created and all related lists are visible.

> **Note:** Starting with Version 13.0.3 of the Policy and Compliance Management application, a **Taxonomy** related list appears. This related list allows you to update an existing taxonomy or map a new taxonomy to the authority document.

### What to do next

Create a citation from the **Authority document** related list.

Related topics

Create or deactivate a citation

### Deactivate an authority document

The **Active** option in an authority document indicates whether the authority documents have been retired.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_compliance.admin or sn_compliance.manager

### Procedure
1. Navigate to **All** > **Policy and Compliance** > **Compliance** > **Authority Documents**.
2. Open an authority document.
3. In the authority document, clear the check box marked **Active**.

   For Authority documents imported from UCF, users are not allowed to clear the **Active** check box as it is a read-only form.

## Manage policy exceptions and extensions

Policy exceptions and extensions provide temporary relief for non-compliant controls.

The policy exception captures the rationale, comments, and evidence to support the acceptance or rejection of a policy exception request. Also, you can request an extension to an approved policy exception before the policy exception validity period. The control owner, the compliance manager, and the risk manager may be involved in the policy exception and extension workflow.

### Request a policy exception

Users can request exceptions for policies, control objectives, or issues by specifying the reason of exception on a particular list of the systems, applications, networks, or entities for which the exception will apply. The user must also specify the duration for which the exception is required.

### Before you begin
Role required: sn_grc.business_user, sn_grc.business_user_lite

### About this task
Exceptions provide temporary relief for users unable to meet compliance requirements due to extraordinary situations. For example, if the user is unable to meet a control that stipulates that all critical OS servers must be patched within 48 hours after the OS vendor releases patches.

### Procedure
1. Navigate to **All** > **Policy and Compliance** > **My Policy Exceptions**.
2. Click **New**.
3. On the form, fill in the fields.

#### Policy Exception form

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Requester | Person requesting the policy exception, usually the control owner. |
| Approval group | Group that has the compliance manager role. You cannot edit the approval group if the policy exception reaches Review state.<br><br>If you do not provide an approval group, then the field defaults to compliance manager. Compliance manager is the default role if the policy exception is raised from any upstream application that is integrated with |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | GRC. For example, if you raise a policy exception for a problem that is related to an incident and that problem is related to GRC. |
| Approver | User from the approval group. If the exception policy moves to the **Analyze** state, then you must select an approver. |
| State | State of the policy exception within the approval workflow. |
| Substate | Approval substate of the policy exception within the approval workflow. |
| Priority | Approval priority of this policy exception |
| Watch list | Users that are notified when the request is updated. |
| Name | Unique name of the policy exception. |
| Reason | Reason for requesting the policy exception. The requester can change the reason until the policy exception is approved. |
| Justification | Statement of explanation for the policy exception. Justification is also displayed in the **Additional comments** field of the **Comments** tab. |
| Source | |
| Source type | Type of policy exception that you want to create. The options are:<br>◦ Policy: Create a policy exception based on a policy.<br>◦ Control objective: Default is a single control objective on which the policy exception is created.<br>When you select a control objective, the**Impacted controls** tab appears, where you can select controls associated to the control objective.<br>◦ Controls: Option to create a policy exception on multiple controls.<br>Select **Control** to associate multiple controls from different control objectives. This option supports multiple controls objectives for your policy exception, instead of creating multiple policy exceptions that could be applied on multiple controls.<br>◦ Issue: Issue associated with this policy exception. |
| Control objective | Control objective associated with this policy exception. |
| Issue | Issue associated with this policy exception. |
| Target record | Target record table on which the policy exception is applied. This table is also referenced in the **Policy exception target table** field of the Policy Exception Integration Registry form. |
| Risk assessment | |
| Risk rating | Select the risk rating as determined by the risk assessment performed on the policy exception. |
| Risk description | Description of the risk as performed by the risk manager during risk assessment. |
| Analysis of risk and impact | Details on the likelihood of this risk occurring and residual impacts of this risk on the policy exception. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Risk mitigation plan | The risk mitigation plan for this policy exception. |
| Schedule | |
| Valid from | Day on which the policy exception begins. |
| Valid to | Day on which the policy exception ends.<br><br>**Valid to** date must be after **Valid from** date and cannot be a past date. |
| Duration | Number of days between the **Valid from** and **Valid to** dates. |
| Approved extensions | Number of times extensions have been requested so far and have been approved. |
| Remaining extensions | Number of times extensions can be requested in future.<br><br>`Remaining extensions = Value in the` *`Number of extensions allowed for a policy exception`* `property – Number of Approved extensions`. |
| Created | Date on which the policy exception was requested. |
| Date approved | Date on which the request was approved. |
| Extension date | Requested extension date, which is after the **Valid to** date. |
| Extension reason | Reason for extension. |
| Original valid to | Date until which the policy exception was originally requested and approved. The original **Valid to** date is populated only when the extension is approved. |
| Comments | |
| Work Notes | Work notes can be used by exception reviewers and approvers to share Information about the exception. |
| Additional comments | These comments are used by the reviewer to communicate additional information to the exception requester. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |

**Note:** In versions prior to Version 10.1, the **Risk assessment** tab was called **Business Impact Analysis** and required that the GRC: Risk Management application be activated. Starting in Version 10.1, the dependency on Risk Management has been removed and the associated field names have changed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Approved extensions**, **Remaining extensions**, **Date approved**, **Extension date**, **Extension reason**, **Original valid to** fields appear only when you have requested an extension on the policy exception and has been approved by the approver.

4. Save the policy exception.
   A series of tabs appear.
5. Click any of the tabs to view the various types of information for the policy exception
6. Click **Update**.

### Request an extension

Request an extension for the policy exception that you created.

### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **My Policy Exceptions**.
2. Open the policy exception for which you want to request extension.

   As a requester you can request extensions to a policy exception that is in Approved state more than once. Configure the *Number of extensions allowed for a policy exception* property to request policy extension multiple times.

   a. To set up the property, navigate to **All** > **Policy and Compliance** > **Administration** > **Properties**

   b. Enter the number in the *Number of extensions allowed for a policy exception* property.
   If you enter 20, then you can request 20 extensions for each policy exception.

   **Note:** If an extension request is rejected by the approver, then you can request another extension until the **Valid to** date is reached.

3. Click the **Request Extension** button.
4. On the pop-up, fill in the **Extension date**, **Extension reason**, and **Justification** fields.

#### Request extension form

| Field | Descriptions |
|---|---|
| Extension date | Requested extension date, which is later than the **Valid to** date. |
| Extension reason | Reason for extension. |
| Justification | Statement of explanation for the request extension. Justification is also displayed in the **Additional comments** field of the **Comments** tab. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Request**.
   You can see the policy extension details in the Schedule tab of the Policy exception form after the requester has requested for an extension and the extension has been approved by the approver.

### Review the policy exception and extension request

After reviewing a policy exception request, a compliance manager can accept or reject the request. However, if the compliance manager doesn't have enough information decide, they can request a risk assessment by the risk manager.

### Before you begin

Role required: compliance manager

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **My Policy Exceptions**.
2. Select the policy exception.
3. Perform one of the following actions.

| Option | Action |
|---|---|
| To view or add impacted controls to the policy exception | **a.** Select the **Impacted Controls** tab.<br>**Note:** You can add a single control objective if your **Source type** is **Control objective**. However, if your **Source type** is **Controls**, then you can select multiple controls from different control objectives. For more information, see Request a policy exception.<br>**b.** Select the **Add** or **Add All** buttonto add the manually created controls.<br>**c.** Choose the controls to associate to the policy exception. |
| To view mitigating controls on the policy exception | Click the Mitigating Controls tab. |
| To view or add risks to the policy exception | Click the Risks tab.<br>**Note:** This option is available when Risk Management plugin is also activated. |
| To view or add approvers to the policy exception | Click the Approvers tab. |
| To request extension | **a.** Click the **Request extension** button.<br>**b.** Select a valid date that is later to the **Valid to** date in the **Extension date** field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Action |
| --- | --- |
| | **c.** Select a reason from the list in the **Extension reason** field.<br>**d.** Enter an explanation for the request extension in the **Justification** field. Justification is also displayed in the **Additional comments** field of the **Comments** tab.<br>**e.** Click **Request**. |

**4.** Perform one of the following actions.

| Option | Action |
| --- | --- |
| To approve the policy exception | Click **Approve**.<br>An email notification is sent to the requester that the PER was approved and goes into effect. |
| To reject the policy exception | Click **Reject**.<br>An email notification is sent to the requester that the PER was rejected and the request is closed. |
| To approve the policy extension | Click **Approve Extension**.<br>An email notification is sent to the requester that the extension request was approved and goes into effect. |
| To reject the policy extension | Click **Reject Extension**.<br>An email notification is sent to the requester that the extension request was rejected and the request is closed. |
| To request a risk assessment on the policy exception | Click **Request Risk Assessment**.<br>An email notification is sent to the risk managers group.<br>**Note:** This option is available when Risk Management is also activated. |
| To request business owner approval | Click **Request Business Owner Approval** . |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Action |
| --- | --- |
| | An email notification is sent to the business owner. |

5. Click **Update**.

### Request a policy exception through Service Portal

Your employees and business users within your company can request a policy exception through the ServiceNow® Service Portal.

#### Before you begin

Role required: sn_compliance.user, sn_grc.business_user, sn_grc.business_user_lite

#### Procedure

1. Navigate to **All** > **Service Portal** > **Service Portal Home**.
2. In the screen header, navigate to **GRC** > **My Policy Exceptions** to view all policy exceptions that you requested.
3. Click **New Policy Exception**.
4. On the form, fill in the fields.
   Complete the Policy Exception form. Specify what the policy exception is for and select appropriate policy, control objective, or issue. This question is for you to identify the appropriate source type.

   When you select a control objective, the **Impacted controls** tab appears, where you can select controls associated to the control objective. You can also search and select an entity.

   Select **Control** to associate multiple controls from different control objectives. This option supports your policy exception for multiple controls objectives, instead of creating multiple policy exceptions that could be applied on multiple controls.

   If you are creating a policy exception from **GRC** > **My Policy Acknowledgements**, then **What is the exception for?** field auto-populates the value as Policy. The name of the policy also appears in the **Policy** field.

   In **Issue** field, you can search by the description and select the appropriate issue.
5. Click **Submit**.

   If you raise a policy exception from Service Portal and if verification rules are not configured, then the policy exception moves to the Analyze state. However, if verification rules are configured for the policy exception, then the policy exception moves to the New state and the verification approval process is triggered. As verification rules are configured the approver is required to verify the policy exception and approve it, only then the policy exception moves to Analyze state.

### Request a policy extension through Service Portal

From the ServiceNow® Portal, anyone who has requested a policy exception can request an extension before the policy deadline.

#### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Add the My Policy Exceptions widget to the Service Portal index page. The widget is visible only if there is at least one policy exception in your list.

### Procedure

1. Click **My Policy Exceptions** in the Service Portal.
2. Open the policy exception for which you want to request for extension.
   The number of remaining extensions that you can request is displayed.
3. In the **Request extension** section, enter the date until which you want to extend.
   A note displays the remaining number of extensions that you can request.
4. Click **Request**.

### Result

The extension request is sent for approval to the approving authority.

#### Policy Exception Integration with Vulnerability Response

Starting with Version 10.1, you can request policy exceptions using the GRC policy exception management capability inherent in the Policy and Compliance Management application from within version 10.3 of the Vulnerability Response application.

## Benefits of using the Policy Exception Integration

Requesting exceptions using the policy exception integration with Policy and Compliance Management provides the following benefits:

- Perform assessments to gather additional information about the requests.
- Request exceptions based on a specific policy or control objective. This action shows the effects on compliance when an exception is approved.
- Configure approvals to be triggered automatically based on the risk rating, policy, or control objective associated with the policy exception.

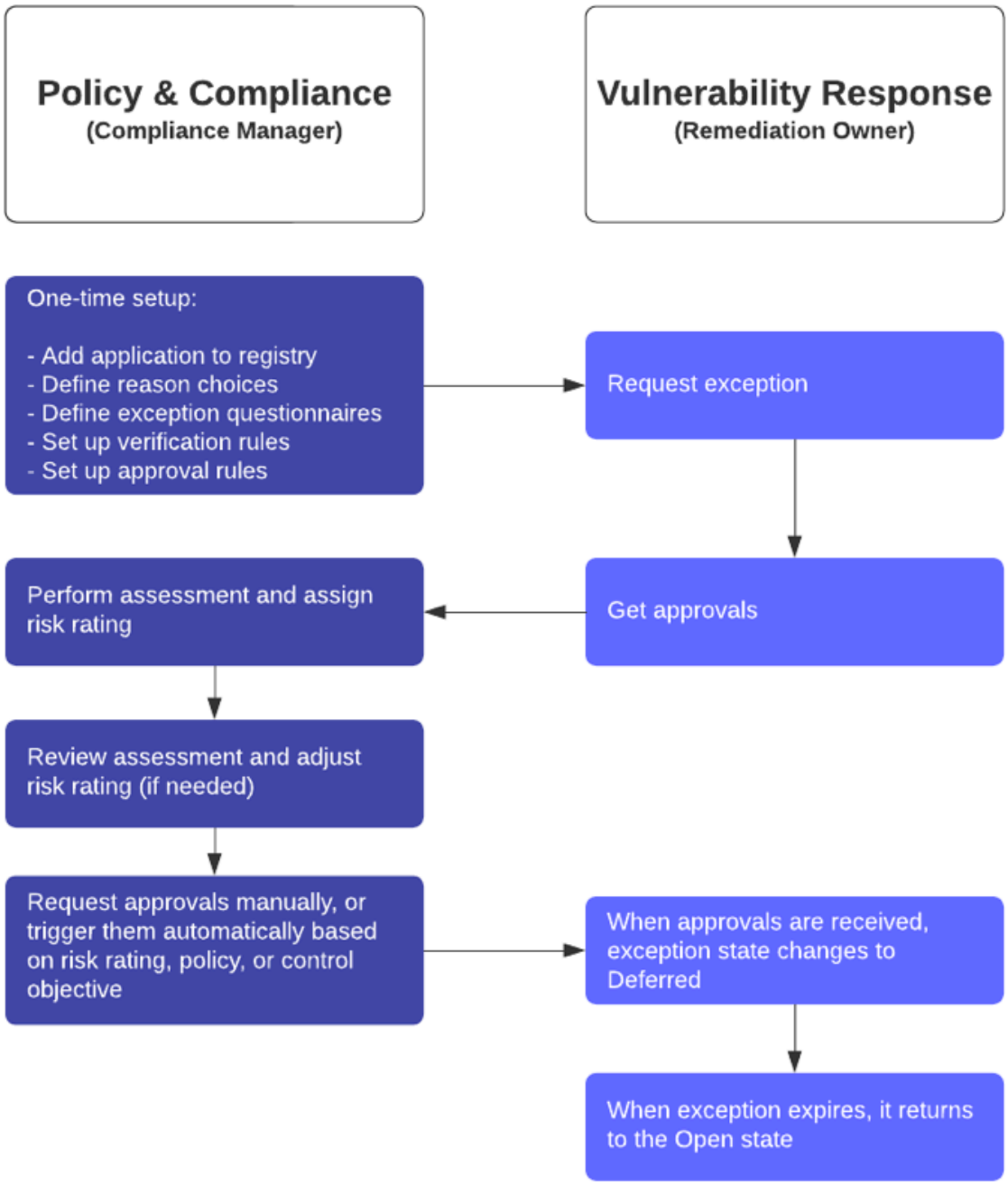
## How the Policy Exception Integration works

The scenario described here assumes that a vulnerability has been identified in your system and your remediation owner has determined that a software patch is needed. The patch has not been fully tested and the owner is requesting a policy exception to defer deployment of the patch until testing is complete.

The following diagram illustrates the steps performed by the compliance manager and the remediation owner in each of the applications.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Policy Exception integration

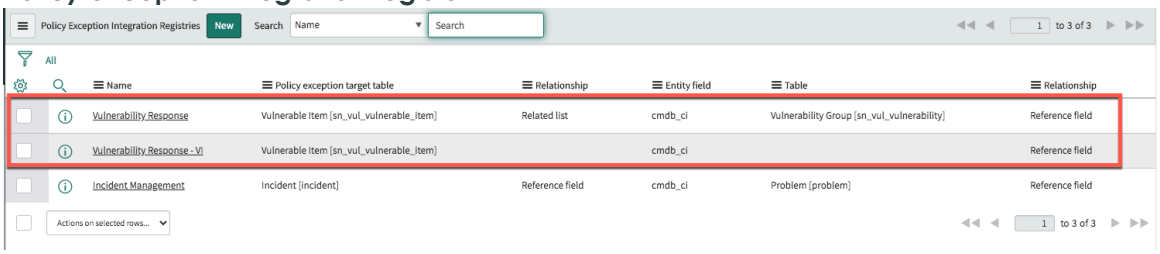



**Note:** The GRC business user (sn_grc.business_user) or business user – lite (sn_grc.business_user_lite) is the minimum required role to raise a policy exception from an upstream application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. When the Vulnerability Response application was installed, two policy exception integration records are automatically created and added to the Integration Registry, one for a vulnerability group and one for a vulnerable item.

**Policy exception integration register**




To configure the vulnerable item record, the compliance manager performs the following steps.

a. Identifies the mapping of tables used to integrate the two applications.

b. Defines reasons for requesting exceptions.

c. (optionally) Defines policy categories for filtering policies

d. (optionally) Creates one or more questionnaires to be sent to the requester to gather additional information about the policy exception request.

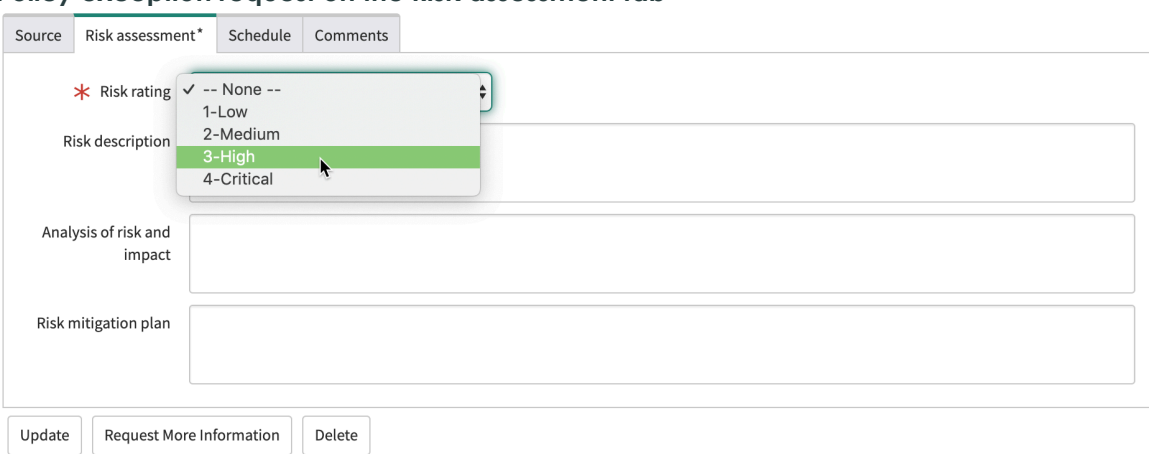
2. The compliance manager also defines optional verification rules and approval rules to automate the process of getting approvals for the policy exception.

3. In Vulnerability Response, the remediation owner Request an exception using GRC: Policy and Compliance Management .

4. If a verification rule was defined for the application, the designated approvers are notified that their approval is required. If any fields in the policy exception request were not filled in by the requester (for example, the Policy or Control Objective), those fields become mandatory for the approvers. When the approvers have reviewed, completed, and approved the request, it transitions to the Analyze state and is assigned to the compliance manager for further analysis and approval.

5. In Policy and Compliance Management, the compliance manager receives the approved request, and assigns a risk rating to the policy exception request on the **Risk assessment** tab.

**Policy exception request on the Risk assessment tab**




When the policy exception record is saved, information in the **Source** tab, including the source application and source record, as well as information in the **Vulnerable Items**

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

related list are auto-populated. The compliance manager now has access to all the data needed to review and approve the policy exception.

6. In Policy and Compliance Management, the compliance manager performs the exception assessment, if assessments were configured. When the assessment is completed, the compliance manager returns to the **Risk assessment** tab and updates the **Risk rating** based on the findings of the assessment, if needed. The compliance manager also populates the following fields with information gathered during the assessment.

**Risk assessment tab**

| Field | Description |
|---|---|
| Risk description | Provide details about the risk associated with this policy exception. |
| Analysis of risk and impact | Provide details about your analysis of the risk and impact to the policy exception. |
| Risk mitigation plan | Provide details about the mitigation plan associated with this policy exception. |

7. If the policy exception is missing any information, the compliance manager can click **Request More Information** and add comments to identify the type of data needed. The requester is notified and provides the requested information.
8. Optionally, the compliance manager can send the policy exception out for an additional in-house review before approving it by clicking **Request Review**.

> **Note:** Prior to requesting a review, ensure that the Impacted Controls related list contains the controls that are impacted by the policy exception. Simply open the related list, click **Add**, and select the controls.

9. If the policy exception is of a particularly high risk, and the compliance manager believes that approval should come from someone higher in the organization (for example, the CIO), the compliance manager can click **Request Approval**.

   Otherwise, approval is performed in the following scenarios.

| Approval rule defined | Effect on approval |
|---|---|
| If an approval rule was not defined for Vulnerability Response | Clicking the **Approved** button causes the policy exception to be approved. |
| If an approval rule was defined, but the **Auto-trigger** check box was not selected | You can click **Request Approval** to send the policy exception to the users or groups defined in the rule. For example, an approval rule may indicate that when the policy exception is based on a particular policy, a certain set of users or groups are notified that they need to provide approval for the policy exception. Or, an approval rule may be defined so that any policy exception with a risk rating of Critical is automatically sent to a certain set of approvers.<br><br>The number of approvers necessary to approve the policy exception depends on the setting in the **Required Approval** field in the rule. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Approval rule defined | Effect on approval |
|---|---|
| | You can also click **Approve** to approve the policy exception yourself. |
| If an approval rule was defined, and the **Auto-trigger** check box was selected | Clicking the **Approve** button causes the approval rule to be executed and the policy exception is automatically sent to the users or groups defined by the rule for approval. Auto-trigger causes this step to be mandatory. When approvals are received, the policy exception goes into effect. |

10. In Vulnerability Response, after the approvals have been received, the policy exception becomes active and the patching activity on the vulnerable item is deferred until the policy exception expires. When the **Valid until** date is reached, the policy exception expires and the state of the vulnerable item changes from Deferred to Open.

## Manage issues in Policy and Compliance Management

You can measure the effectiveness of your company's risk management program by how quickly and completely it identifies and reacts to compliance issues.

To know more about how issues function across all GRC applications, see GRC issues.

### Manually create GRC issues

As a GRC user, you can manually create issues to document policy, risk, or audit observations, or to accept any GRC problems. You can also identify the source of the issue to help analyze and classify the issues.

#### Before you begin

Role required: (per product)

- In Policy and Compliance Management: compliance_admin, compliance_manager, sn_compliance.user, sn_grc.business_user, sn_grc.business_user_lite
- In Risk Management: risk_admin, risk_manager, or sn_risk.user
- In Audit Management: audit_admin, audit_manager, audit_admin, or sn_audit.user

**Note:** Starting with Version 12.0.1 of the products mentioned above, the minimum role for the **Assigned to** user on the Issues form is GRC Business User [sn_grc.business_user]. The minimum role for the **Issue manager** is GRC User [sn_grc._user].

For more information on the access control limitations to issues, see GRC business user role to control access and track usage of compliance tables.

#### Procedure

1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Issues** > **Create New**.
   - **Risk** > **Issues** > **Create New**.
   - **Audit** > **Issues** > **Create New**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** Starting with Version 12.0.1 of the products mentioned above, the minimum role for the **Assigned to** user on the Issues form is GRC Business User [sn_grc.business_user]. The minimum role for the **Issue manager** is GRC User [sn_grc._user].

2. On the form, fill in the fields.

**Issue form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Assignment group | Group to which this issue has been assigned. Each member gets a notification when an activity happens on this issue. |
| Assigned to | Member of the group assigned to resolve the issue.<br><br>Starting with Version 12.0.1, the user must have at least the sn_grc.business_user role.<br><br>**Note:** Use the bulb icon to get suggestions on who must the issue be assigned to. The bulb icon only appears if you have the GRC: Predictive Intelligence application activated, the form is saved, the **Assigned to** field is not inactive, and the GRC Property is selected as Similarity Analysis. For more information, see .<br><br>You can configure a hierarchy of users to access the issue record. For more information, see User hierarchy access control for issue and remediation task records.<br><br>Starting with Version 12.0.1, the assigned-to user gets an email notification when the issue manager requests more information.<br><br>Starting with Version 12.0.1, when an issue transitions to the **Respond** state, an entry in the **Assigned to** field is mandatory. |
| Issue source | Source from where the issue was created. This field is auto-populated with one of the following options based on how the issue is created:<br>◦ Indicator Failure: Issue is created by a failure of the indicator<br>◦ Risk Assessment: Issue is created in a risk<br>◦ Risk Event: Issue is created in a risk event |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Control Attestation Failure: Issue is created due to a non-compliant control<br>◦ Control Test Failure: Issue is created when a control is ineffective and the control test is marked as closed and complete<br>◦ Ad-hoc: Issue is manually created |
| Issue type | Type of issue. Choices are:<br>◦ Control design effectiveness failure<br>◦ Control operative effectiveness failure<br>◦ Control does not meet requirement<br>◦ Control does not exist<br>◦ Non-compliance to a regulation<br>◦ Non-compliance to a policy<br>◦ Improvement or suggestion to an existing policy<br>◦ Recommendation for a new policy<br>◦ Process optimization or improvement<br>◦ Observation<br>◦ Data Breach<br>◦ Fraud<br>◦ Misstatement<br>◦ Training<br>◦ Documentation<br>◦ Risk issue<br>◦ Other |
| Classification | The classification of the issue as a risk, compliance, or audit, based on the issue type. |
| Issue manager group | The group responsible for managing and reviewing the issue.<br>Starting with Version 12.0.1, the following enhancements and requirements were introduced:<br>◦ Members of the issue manager group must have one of the following roles:<br>▪ sn_audit.manager<br>▪ sn_audit.user<br>▪ sn_compliance.manager<br>▪ sn_compliance.user<br>▪ sn_grc.manager |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ▪ sn_grc.user<br>▪ sn_risk.manager<br>▪ sn_risk.user<br>◦ When an issue transitions to the **Analyze** state, an entry in either the **Issue manager group** or **Issue manager** field is mandatory.<br>◦ When an issue is assigned to the group, the members receive an email notification. Additionally, the issue manager receives an email notification when the issue transitions to the **Review** state. |
| Issue manager | The user responsible for managing and reviewing the issue.<br>Starting with Version 12.0.1, the following enhancements and requirements were introduced:<br>◦ The issue manager must have at least the sn_grc.user role.<br>◦ The issue manager receives an email notification when the assigned-to user provides requested information.<br>◦ When an issue transitions to the **Analyze** state, an entry in either this field or **Issue manager** is mandatory.<br>◦ When an issue transitions to the **Respond** state, an entry in this field is mandatory. |
| State | ◦ New<br>◦ Analyze<br>◦ Respond<br>◦ Review<br>◦ Closed Complete<br>◦ Closed Incomplete |
| Substate | The substate and applicable details for the substate. |
| Priority | The sequence in which an issue must be resolved, based on its impact and urgency:<br>◦ **1 — Critical**<br>◦ **2 — High**<br>◦ **3 — Moderate**<br>◦ **4 — Low**<br>◦ **5 — Planning** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Issue rating | Starting with Version 12.0.1, the issue manager can assign the issue rating to the issue. Based on the issue rating, the **Due date** under the **Dates** tab is calculated as follows and displayed:<br>◦ Very high (2 days)<br>◦ High (4 days)<br>◦ Moderate (8 days)<br>◦ Low (10 days)<br>◦ Very Low (15 days)<br>You can manually override the **Due date**.<br>**Note:** Users with the sn_grc.manager and sn_grc_advanced.issue_triage_manager role can navigate to **Policy and Compliance** > **Administration** > **Issue rating** and define additional issue ratings.p<br>When the issue transitions to the **Respond** state, the Issue rating field is read only. |
| Issue group rule | Group rule assigned to this issue. The Issue group rule is used to group similar issues together into a parent issue based on the conditions defined in the rule. This rule enables you to work on similar issues simultaneously and close out the parent issue after all issues are resolved. This closes out all the child issues. |
| Parent Issue | Parent issue this issue belongs to. |
| Configuration item | Item associated with this issue. If all child issues have the same configuration item, it gets copied over to the parent issue |
| Location | Location where the issue occurred. |
| Short description<br>Starting with Version 12.0.1, this label was changed to **Name**. | A name for the issue. |
| Description | A more comprehensive description of the issue. |
| Details | |
| Control/Risk | Control or risk associated with the issue.<br>When the control is associated, the corresponding entity of the control |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | is added to the **Entity** field, and the control objective is added to the **Control Objective/Risk Statement** field. These control objective and entity are the ones that are linked to this control.<br><br>When the control is associated to the issue form, an m2m record is created in the source [sn_grc_m2m_issue_item] table. Whenever a record is added in the source table, a corresponding record, Issue to Entity is added in the destination [sn_grc_m2m_issue_to_entity] table, and another record Issue to Content is added in the destination [sn_grc_m2m_issue_content] table for the associated entity and control objective of the control. |
| Entity | Related entity. |
| Policy | The policy associated with the issue. |
| Authority document | The authority document associated with the issue. |
| Control Objective/Risk Statement | The control objective or risk statement related to this issue. |
| Recommendation | Resolution actions recommended by the risk, compliance, or audit teams. |
| Action Plan | The plan for remediating the issue. |
| Dates | |
| Planned start date | Date and time that work on the issue is expected to begin. |
| Planned end date | Date and time that work on the issue is expected to end. |
| Planned duration | Estimated amount of work time for the issue. |
| Confirmed date | (Starting with Version 12.0.1) The date when the issue is confirmed. This field is read-only, and displays today's date when the issue is moved from **New** to any of the following states:<br>◦ **Analyze**<br>◦ **Review**<br>◦ **Respond**<br><br>**Note:** If a triage issue is converted to an actual issue, this field displays the date it was converted. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Due date | (Starting with Version 12.0.1) This date is auto-populated based on a GRC property. Navigate to **Policy and Compliance** > **Administration** > **GRC Properties**. If the **Auto populate due date based on issue rating** property is set to **Yes**, this field is auto-populated based on the predefined remediation time frame for the issue's risk rating. Otherwise, you can manually enter a due date.<br><br>When an issue transitions to the **Respond** state, an entry in this field is mandatory. |
| Actual start date | Time when work began on this issue. |
| Actual end date | A read-only value that is determined by the **Actual duration** input field. |
| Actual duration | Amount of work time. |
| Created | The date and time the issue was created. |
| Closed | The date and time the issue was closed. |
| Engagement | |
| Engagement | The related engagement. |
| Activity | |
| Additional comments (Customer visible) | Public information about the issue. Click **Post** to add your comments to the issue. |
| Work notes | Click the **Work notes** check box to display the **Work notes** field. Information about how to resolve the issue, or steps already taken to resolve it, if applicable. Work notes are visible to users who are assigned to the issue. Click **Post** to add your work notes to the issue. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on the confidential option, see Confidentiality flag for audit and compliance records. |
| Risk Event | |
| Risk event | The related risk event. |

3. Save the issue record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The tabs at the bottom of the screen enable you to perform various tasks for remediating the issue. You can add policy exceptions and create remediation tasks. Additionally, you can view other issues, indicator results, and task SLAs related to the issue.

**Note:** Starting with Version 12.0.1, the **Task SLA** tab creates and displays SLAs based on the **Due date**. Notifications are sent to the issue owner and issue manager when the issue **Due date** reaches 50%, then 75%, then when it breaches. If the **Assigned to** and **Due date** fields are not empty and the issue is not in the **New** state, an SLA is created for the issue.

If the due date for the SLA changes, a new SLA is created. The SLA is completed when the issue transitions to **Closed Complete** or **Closed Incomplete**. Also, the SLA is cancelled if the **Due date** or **Assigned to** fields are empty, or the state is New.

Also starting with Version 12.0.1, remediation tasks can be created with the Assigned to user and issue manager user roles, as well as any user with the GRC Business User role.

### Group similar issues under a new parent issue

When you are creating an issue, you have the option of grouping the issue with other similar issues.

#### Before you begin

Role required: (per product)

- In Policy and Compliance Management: compliance_admin, compliance_manager, or sn_compliance.user
- In Risk Management: risk_admin, risk_manager, or sn_risk.user
- In Audit Management: audit_admin, audit_manager, audit_admin, or sn_audit.user

#### About this task

Grouping issues under a parent can save you valuable time. For example, assume you have an issue related to patching Windows servers. Since each server is a separate entity, all controls associated with "Windows servers should be patched every Tuesday" will have the same issue. Therefore, the issue can be resolved once for all of the Windows servers by applying the relevant patch one time. So, this feature can be used to group similar issues and resolve them all at the parent level.

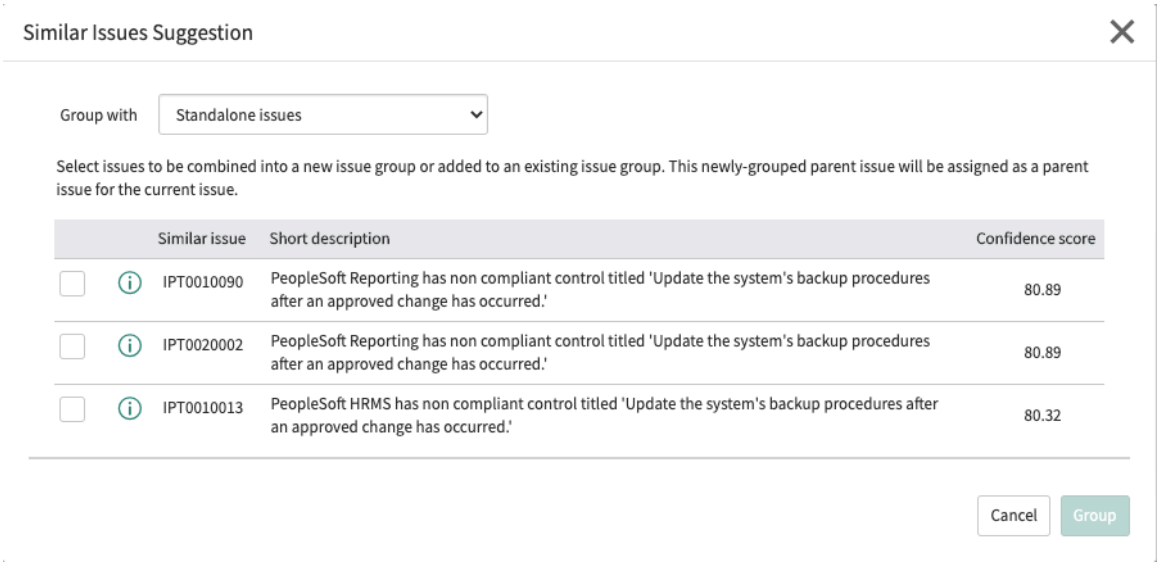
#### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Issues** > **Create New**.
   - **Risk** > **Issues** > **Create New**.
   - **Audit** > **Issues** > **Create New**.
2. On the form, locate the **Parent issue** field.




3. Click the bulb icon ( ) to view similar issues that you may want to assign to this parent issue.

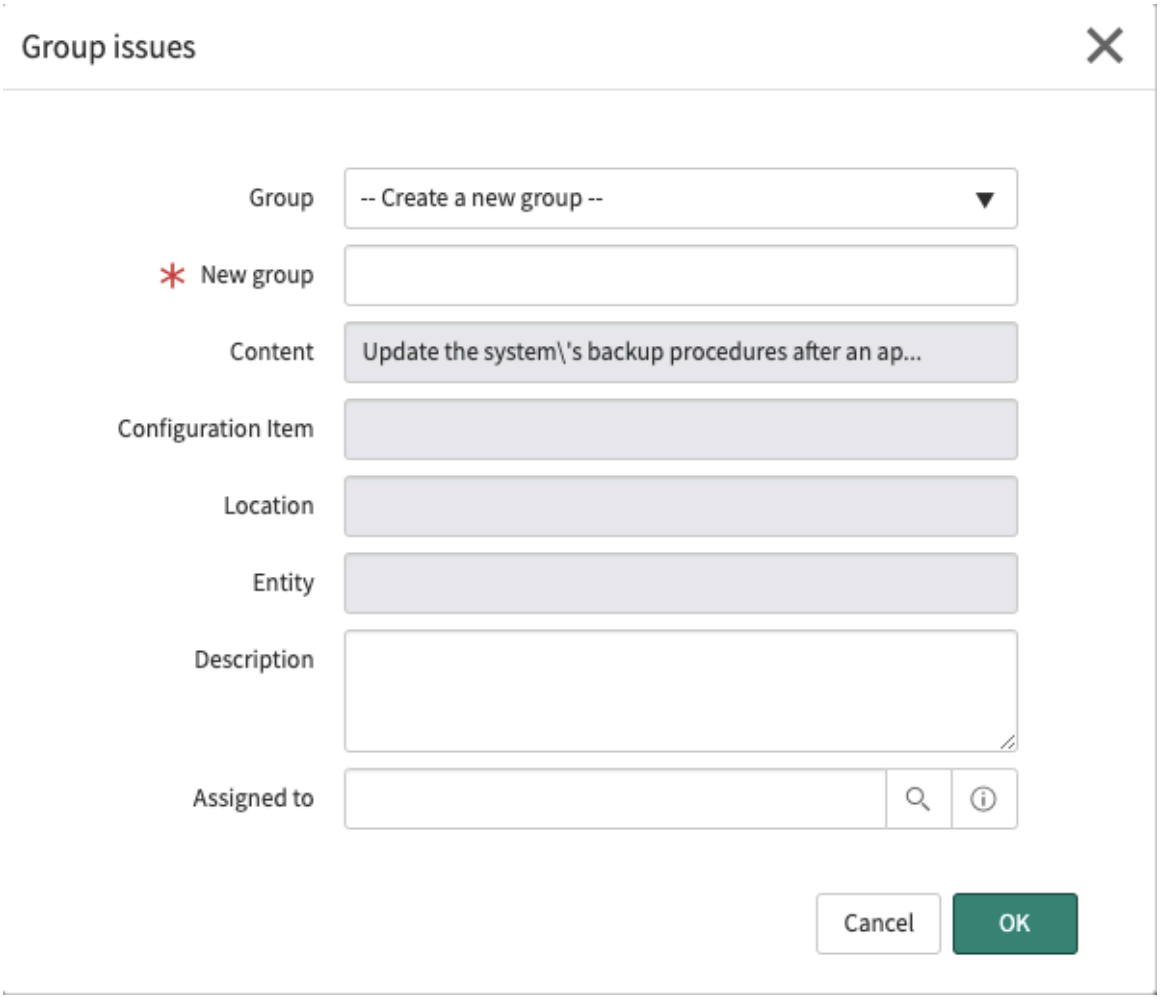
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**Note:** Standalone issues are similar to the current issue, but that are not assigned to a parent issue group. The Confidence score is calculated using a similarity definition included in the GRC: Predictive Intelligence application base system.

4. You can click the Information icon to view details for any similar issues in order to help determine whether they should be grouped with the current issue.
5. Select the similar issues you want to group with the current issue, and click **Group**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




6. On the form, fill in the fields.

**Issue form**

| Field | Description |
|---|---|
| Group | To group the selected issues and assign them to a new group, select **Create a new group**.<br><br>To add the selected issues to an existing group, select the group. |
| New group | This field displays only if you selected **Create a new group**. Type the name of the new group. |
| Description | This field displays only if you selected **Create a new group**. Type a description of the group. |
| Assigned to | This field displays only if you selected **Create a new group**. Select the user to whom the group is assigned. |

7. Click **OK**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The selected issues are added to a new or existing group.

8. You can view the issue in the group by clicking the **Issues** tab.

### Group similar issues under an existing parent issue

When you are creating an issue, you have the option of grouping the issue with other similar issues as part of an existing parent issue group.

#### Before you begin

Role required: (per product)

- In Policy and Compliance Management: compliance_admin, compliance_manager, or sn_compliance.user
- In Risk Management: risk_admin, risk_manager, or sn_risk.user
- In Audit Management: audit_admin, audit_manager, audit_admin, or sn_audit.user

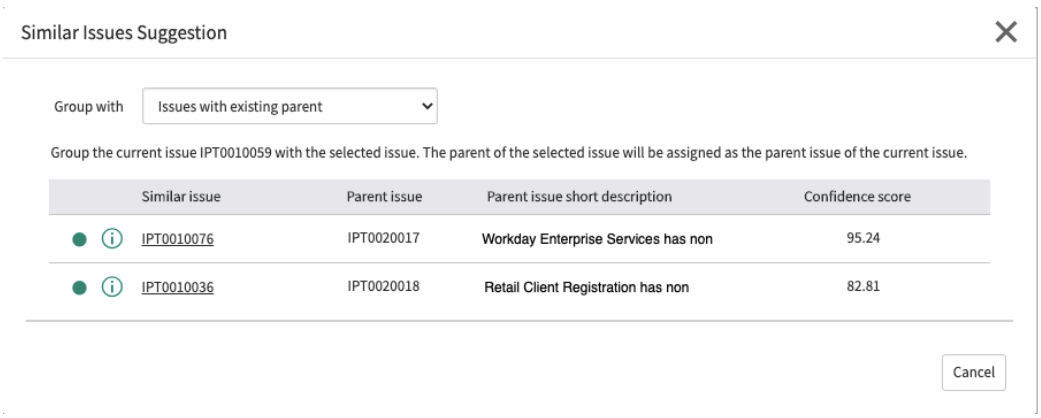
#### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Issues** > **Create New**.
   - **Risk** > **Issues** > **Create New**.
   - **Audit** > **Issues** > **Create New**.
2. On the form, locate the **Parent** field.




3. Click the bulb icon ( ) and select **Issues with existing parent** from the **Group with** drop-down list.

   You are shown a list of similar issues.




4. Click the **Similar issue** you want to group with the current issue.
   The parent issue of the issue you select becomes the parent issue of the current issue.
5. You can view the issue in the group by clicking the **Issues** tab.

### User hierarchy access control for issue and remediation task records

If a user is assigned to an issue or a remediation task, then the manager of the user and the manager above in the hierarchy also get access to the issue or remediation task record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The user reference in the **Assigned to** field, **Opened by** field, or **Owner** field are configurable in the User hierarchy configurations [sn_grc_user_hierarchy_configuration] table. Therefore, you can configure the fields in the table and enter the user reference, for example **Assigned to** or **Issue Manager** as User reference field 1 or User reference field 2. However, you can configure only two fields in a table.

The manager of the user in the user reference field and the manager above in the hierarchy can be configured as User hierarchy field 1 and User hierarchy field 2, respectively. If one of them is no longer the manager of the user in the user reference field, then that user in the hierarchy loses access to the record. You can view the hierarchy of users in the User Hierarchy [sn_grc_user_hierarchy] table.

The prerequisites to enable user hierarchy access control are:

- Users in the hierarchy must have at least the GRC business user (sn_grc.business_user) role.
- The *sn_grc.enable_user_hierarchy_access_control* system property must be set as **true**.

The concept of user hierarchy is helpful as it provides more visibility to the users in the hierarchy in tracking its completion when it is assigned to a user in a team. User hierarchy fields are not visible in the Issue or Remediation task form, however internally this feature enables you to restrict access to records based on those users in the hierarchy who can access them.

### Report self-identified issues via the Service Portal

Your employees and business users within your company can self-identify an issue and submit it via the ServiceNow® Service Portal. Following submission, a triage issue is automatically created.

#### Before you begin

You must download the GRC: Advanced Core application before you can use the Issue Triage featuring within Policy and Compliance Management. For more information, see Download a GRC application from the ServiceNow Store for the first time.

Role required: sn_compliance.user, sn_grc.business_user, sn_grc.business_user_lite

#### About this task

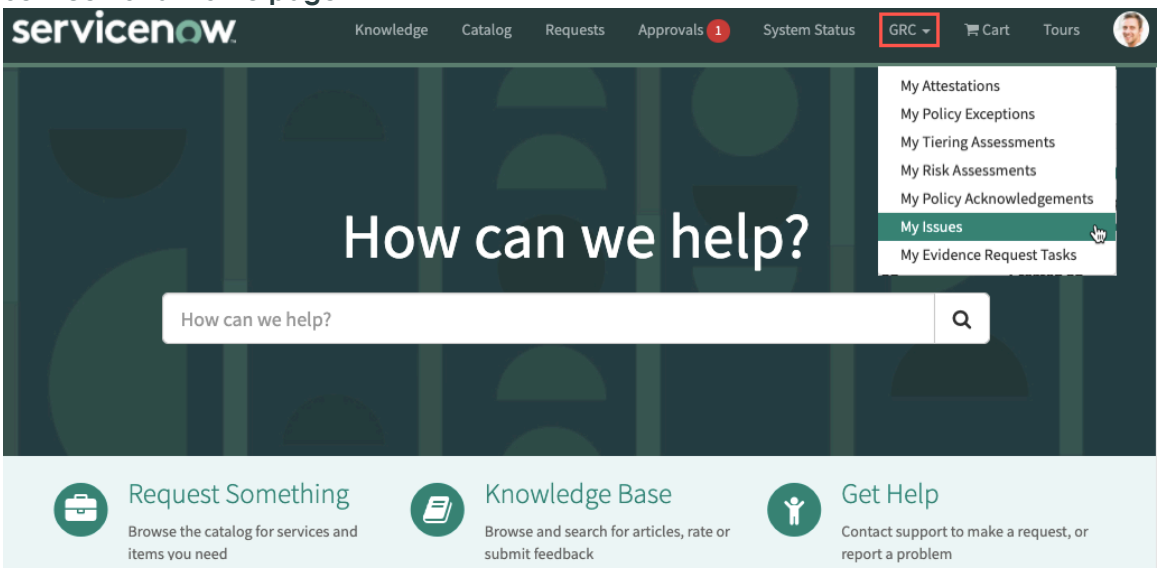
There are multiple methods you can use to report an issue using the Service Portal. For example, you can click the **Request Something** button on the Service Portal home page, select the **Governance, Risk, and Compliance** category, and then click **Report Issue**. An alternate, and perhaps simpler, method is described here.

#### Procedure

1. Open the Service Portal.
   a. In your instance URL, type sp after your instance name.
   b. Press the Return key.

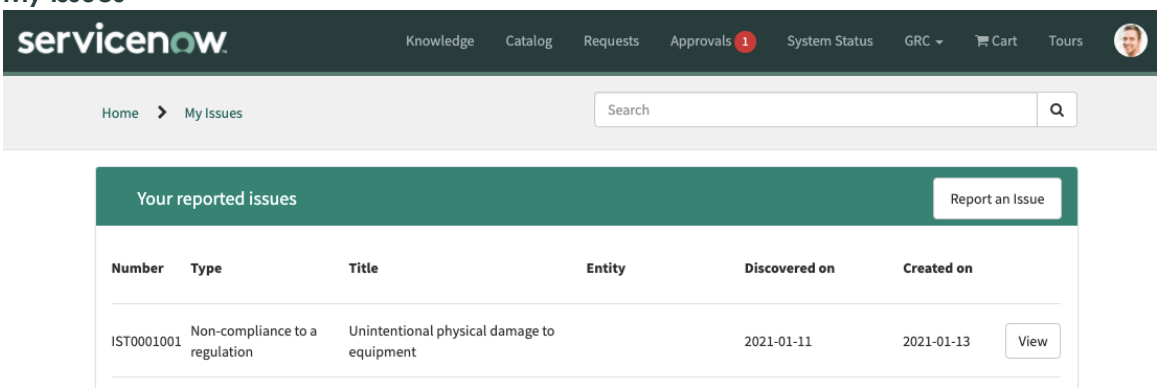
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Service Portal home page**



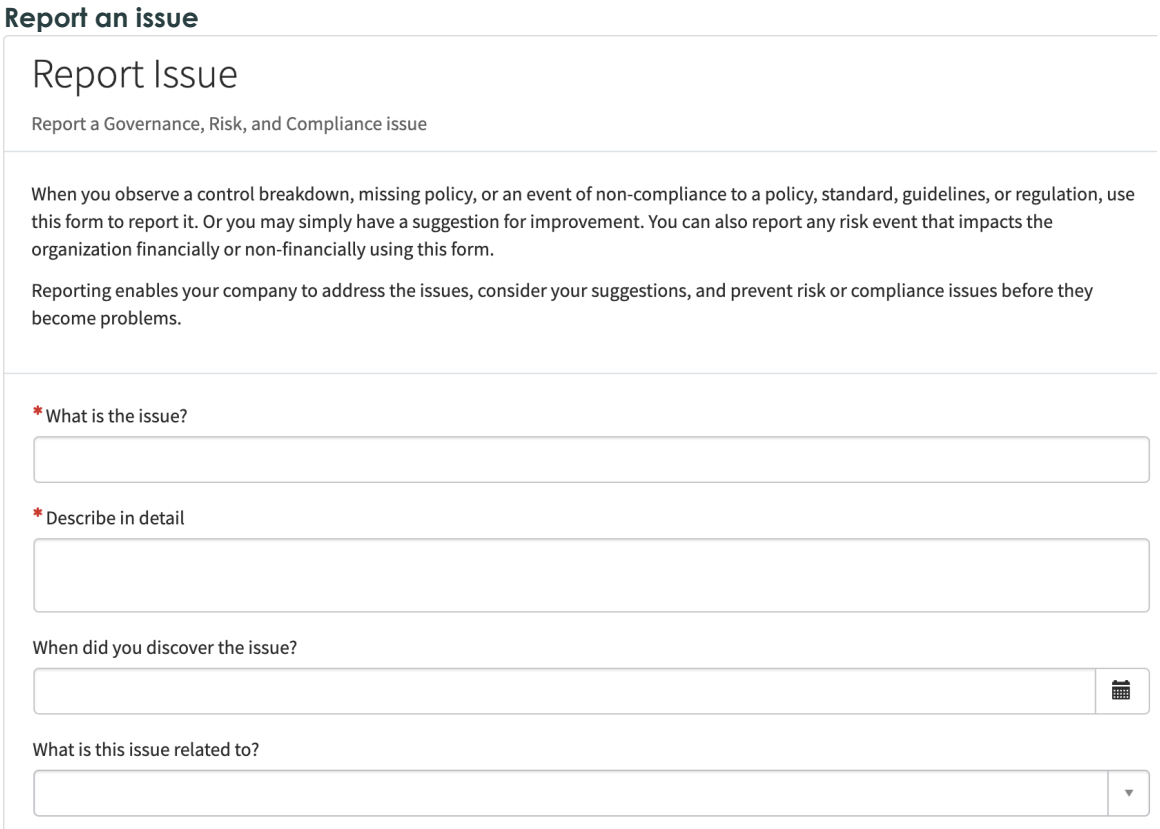

**2.** In the screen header, navigate to **GRC** > **My Issues** to view issues already assigned to you.

**My issues**




**3.** Click **Report an Issue**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




4. Answer the questions presented.

   **Example**
   Additional questions may appear depending on the answers you provide. For example, if your response to the **What type of issue is this?** field is **Incident or loss event**, additional questions relating to the incident or loss event are presented to you. Or if you select **Non-compliance to a policy** at that field, you are asked for the affected policy and what you consider to be the root cause of the issue.

5. When you have completed all of the questions, click **Submit**.

   The request is submitted, and an issue triage record is created. This kicks off the issue triage process.

   **Note:** You can control the options displayed in the Service Portal **GRC** option menu by returning to your instance and navigating to **Policy and Compliance** > **Issue Triage** > **Administration** > **Properties**, and setting the **sn_grc_advanced.enable_my_issues_hide_my_reported_issues** property.

   If it is set to **Yes**, the **GRC** > **My Issues** menu option is available, and the **My Reported Issues** option is hidden. You can use the **My Issues** menu option to create risk or compliance issues that must be triaged before being released as actual issues.

   If the property is set to **No**, the **GRC** > **My Reported Issues** menu option is available, and the **My Issues** option is hidden. You can use the **My Reported Issues** menu option to create actual risk or compliance issues directly from the Service Portal.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Triage a self-identified issue

After an issue has been identified and submitted by employees or business users via the Service Portal, the issue triage process begins. The actual problem is identified and assigned to the appropriate owner for prioritization and resolution.

## Before you begin

Role required:

- sn_compliance.manager
- sn_compliance.user
- sn_grc_advanced.issue_triage_manager
- sn_grc_advanced.issue_triage_user

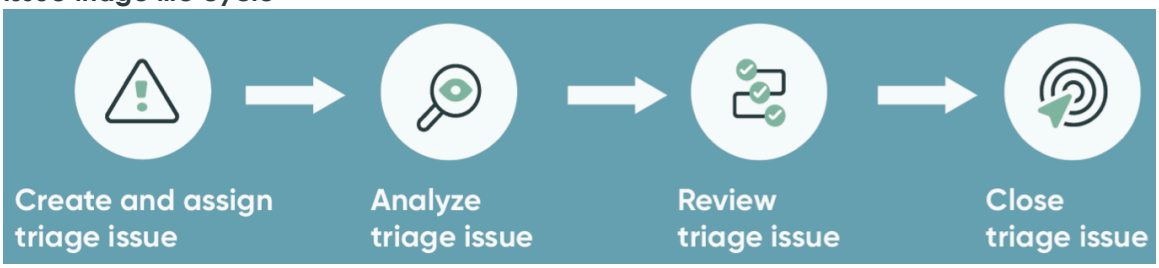
## About this task

The assigned triage teams identify whether the self-identified issues are actual reported issues, risk events, or observations to be tracked and possibly closed out as noise.

**Note:** In the initial release, only self-identified issues are handled by the triage process. In a later release, system-generated issues, such as those caused by indicator or attestation failures, will also be triaged.

The end-to-end flow of the issue triage life cycle is illustrated and described here.

**Issue triage life cycle**




| Stage | Description |
|---|---|
| Create and assign triage issue | An employee identifies an issue related to an entity, control, policy, authority document, process, or risk, and submits a triage request in the ServiceNow Service Portal.<br><br>Based on the type of issue submitted and an issue assignment rule, the issue is assigned to a triage team and a triage owner. |
| Analyze triage issue | The triage team decides whether the issue should be analyzed as an actual issue or risk event, or tracked as a recommendation for a policy or for optimizing a process.<br><br>During analysis, the triage team may request more information from the issue creator. The team may also optionally send the issue to the compliance manager, risk manager, or triage manager with a triage result.<br><br>Possible results include: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Stage | Description |
|---|---|
| | • Confirmed as a new issue<br>• Confirmed as an existing issue<br>• Confirmed as a risk event<br>• Track as a recommendation<br>• Close as a non-issue/No action required |
| Review triage issue | The Review state is optional. The team may send the issue and result to the compliance manager, risk manager, or triage manager for review. They may also request more information from the triage owner.<br><br>The compliance manager, risk manager, or triage manager decides whether the issue should be confirmed as an issue or risk event, tracked as a recommendation, or closed as a non-issue. |
| Close triage issue | If the issue had been determined to be an actual issue or risk event, those records are created, or the triage issue is added to an existing issue.<br><br>When the triage process is completed, the triage issue is automatically closed. The issue can also be manually closed by the manager and triage team. |

The following user roles are involved in the issue triage process.

### Issue triage personas

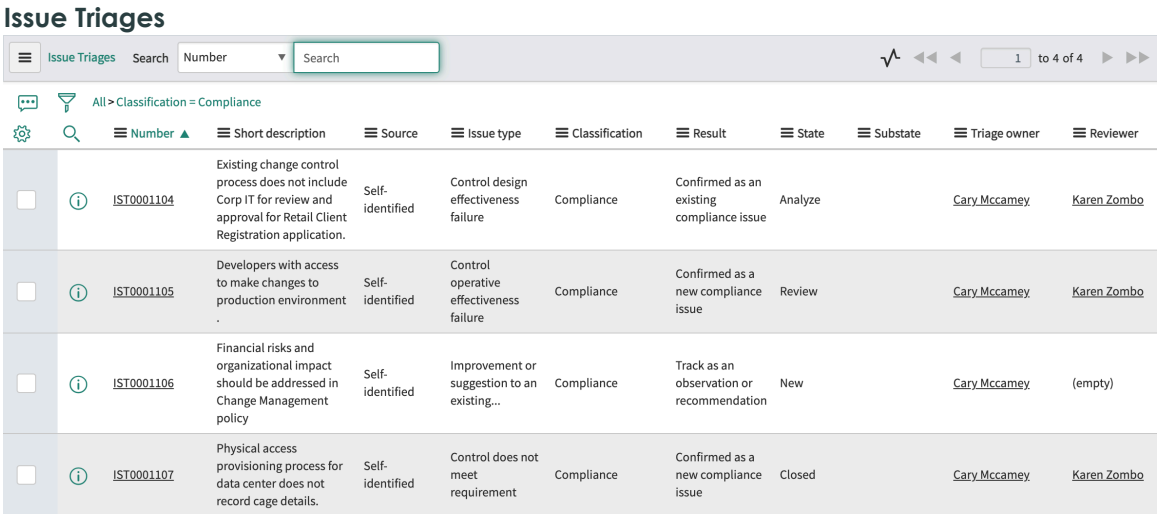
| Persona/Role | Description |
|---|---|
| Business user/Employee | Ability to report issue. |
| • Compliance user/manager<br>• Risk user/manager<br>• Triage user/manager | Ability to triage and review issues |
| Issue manager | Ability to manage and review the reportable issue |
| Issue owner | Ability to resolve the reportable issue assigned to them |

**Note:** The triage user/manager and Issue manager roles were introduced in GRC: Policy and Compliance Management version 11.1.0.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

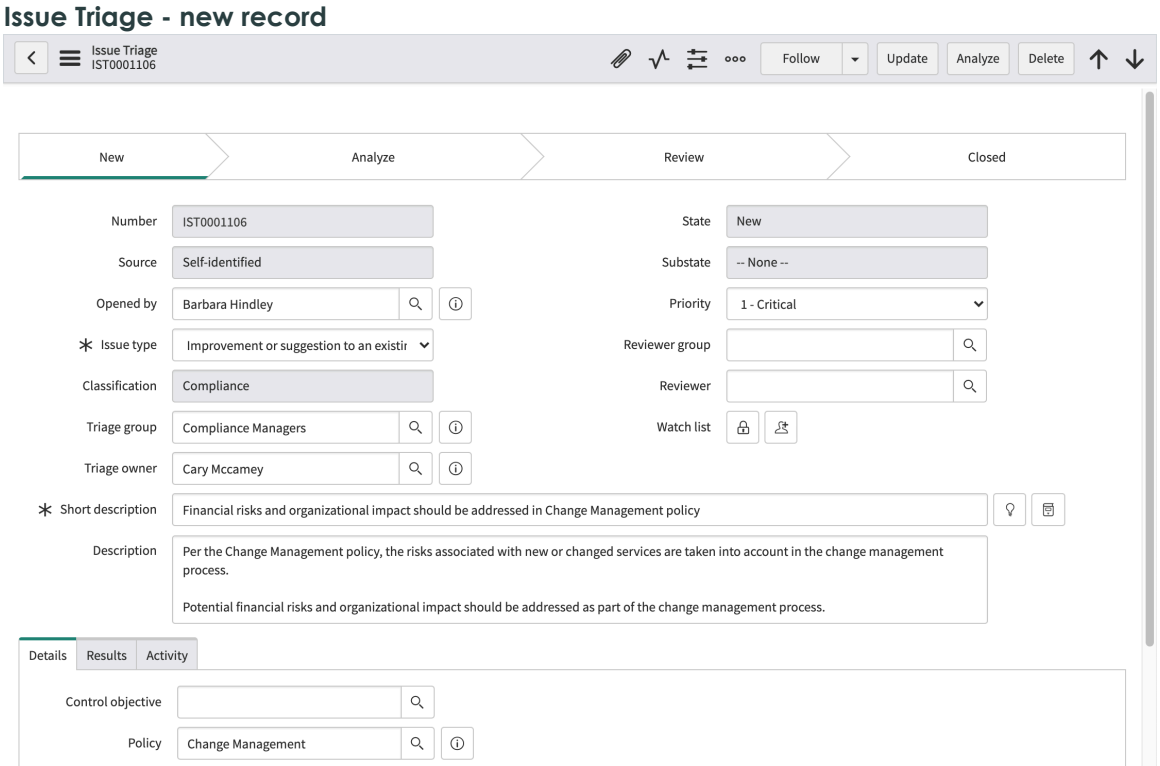
## Procedure

1. Navigate to **All** > **Policy and Compliance** > **Issue Triage** > **My Triage Issues** or **Risk** > **Issue Triage** > **My Triage Issues**.
   The list shows triage issues previously created and assigned to you.




| Number | Short description | Source | Issue type | Classification | Result | State | Substate | Triage owner | Reviewer |
|---|---|---|---|---|---|---|---|---|---|
| IST0001104 | Existing change control process does not include Corp IT for review and approval for Retail Client Registration application. | Self-identified | Control design effectiveness failure | Compliance | Confirmed as an existing compliance issue | Analyze | | Cary Mccamey | Karen Zombo |
| IST0001105 | Developers with access to make changes to production environment . | Self-identified | Control operative effectiveness failure | Compliance | Confirmed as a new compliance issue | Review | | Cary Mccamey | Karen Zombo |
| IST0001106 | Financial risks and organizational impact should be addressed in Change Management policy | Self-identified | Improvement or suggestion to an existing... | Compliance | Track as an observation or recommendation | New | | Cary Mccamey | (empty) |
| IST0001107 | Physical access provisioning process for data center does not record cage details. | Self-identified | Control does not meet requirement | Compliance | Confirmed as a new compliance issue | Closed | | Cary Mccamey | Karen Zombo |

2. Click the number of the issue that you want to triage.

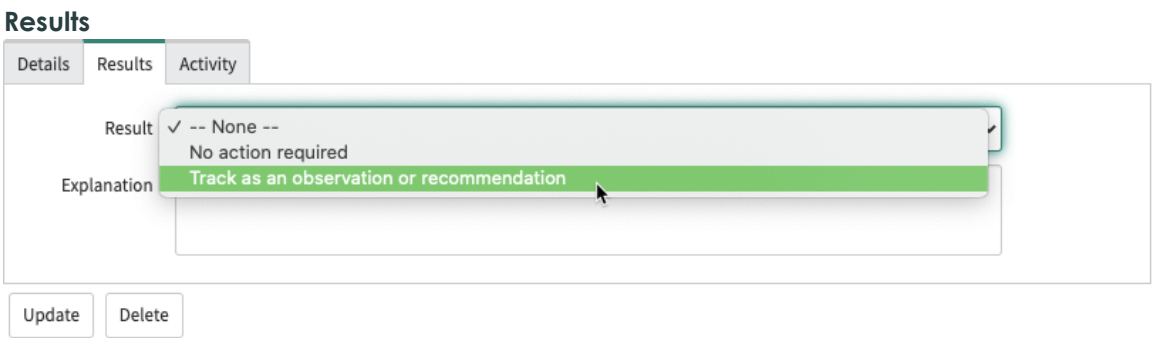



**Note:** The **Classification** field is automatically pre-filled based on the **Issue type** selected. Similarly, an assignment rule called sn_grc_advanced_issue_triage runs and pre-fills the **Triage group**. This rule uses the **Source** and **Classification** to determine the group to which the triage is assigned. Assignment rules also handle issue triages in Risk Management and triages where the **Classification** is set to **Other** (that is, it is initially unknown). For the second use case, you must manually set the **Triage group** to **Risk** or **Compliance**.

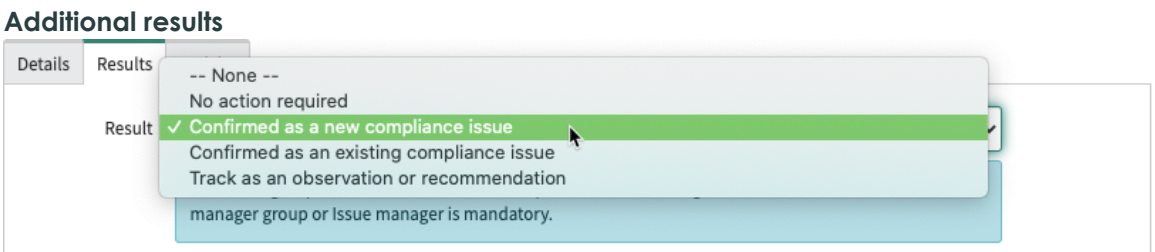
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. When you are ready for triage of this issue to begin, select a **Triage owner** and click **Analyze**.
   The assigned Triage owner can now open the issue and begin analyzing the issue.
4. During analysis, the triage owner can perform several tasks.

   **Example**
   The owner may, for example, decide that the issue is misclassified and can change the **Issue type**. This action could result in the Triage group and Triage owner changing. In this example, the assignment rule runs in the background and the issue is removed from the current owner's queue.
5. The triage owner can also perform the following actions:
   - Click **Request Information** to request additional information from the issue submitter.
   - Click **Request Review** to request a review from the user identified in the **Reviewer** field. That user can open and review the issue by navigating to **Policy and Compliance** > **Issue Triage** > **My Pending Reviews**.
   - Select the **Details** related list to provide additional enrichment to the issue.
6. After it has been determined what action (if any) should be performed on the issue, the triage owner can select a result of the analysis from the **Results** related list.



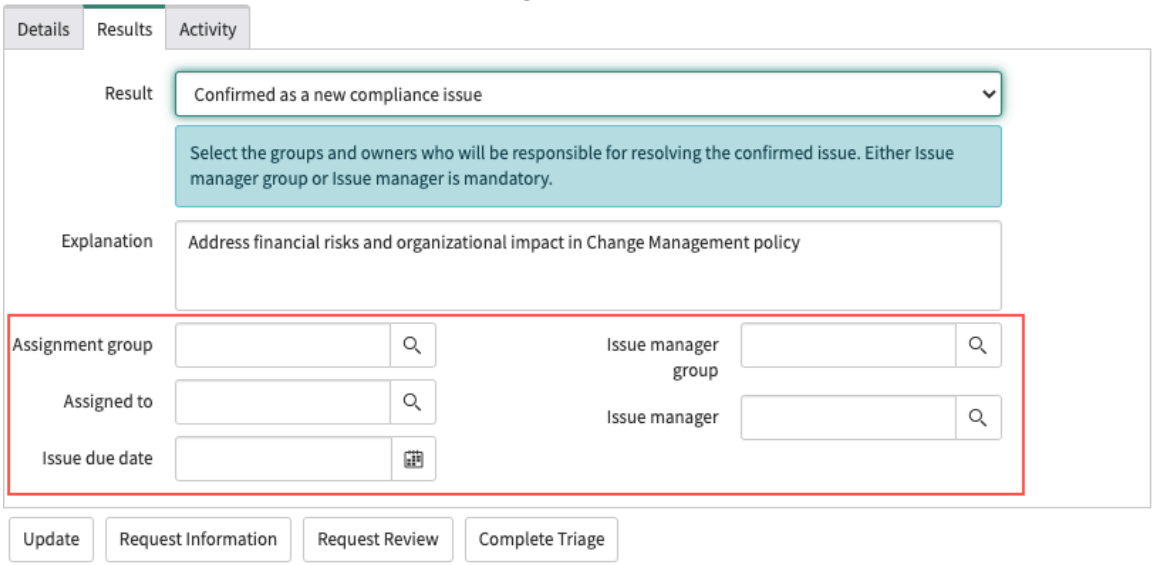

**Note:** The options available in the **Result** field depend on the **Issue type** identified for this issue. For example, if you select **Control design effectiveness failure** as the **Issue type**, the following results may be selected.




7. If you select a result, such as **Confirmed as a new compliance issue**, which requires more action than simple observation, additional analysis fields display, as shown in the following screen.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Additional fields displayed after selecting Result**



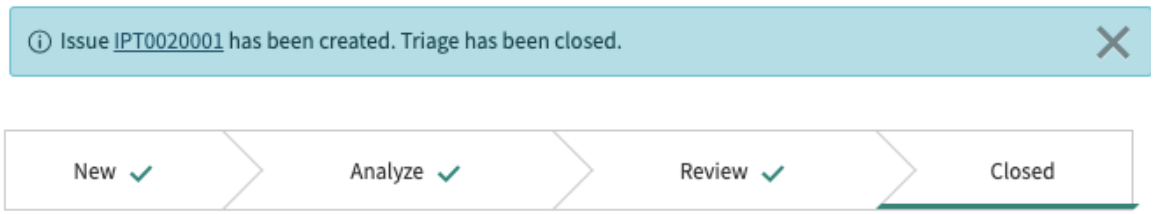

If the result is **Confirmed as an existing compliance issue**, then an **Existing issue** field appears where you must identify the existing issue that you are referring to.

8. When the issue triage is complete, the triage owner can click **Complete Triage**.

   **Note:** If the issue is out for review, the reviewer can also click **Complete Triage** to complete the triage and create an actual issue.

   The issue triage transitions to the **Closed** state and a link to the issue displays at the top of the screen.

**Triage closed and new issue created**




9. The issue can be analyzed using the usual issue management procedures.
   One significant change on the **Issue** form is the addition of an **Issue Triages** related list. Opening the triage record provides the analyst with the details of the triage that resulted in the creation of this issue.

### Remediate an issue in Policy and Compliance Management

After an issue has been identified, triaged, and investigated, you can remediate it.

**Before you begin**
Role required: compliance_admin, compliance_manager, sn_compliance.user, sn_grc.business_user, sn_grc.business_user_lite

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** Starting with Version 12.0.1, the minimum role for the **Assigned to** user on the Remediation task form is GRC Business User [sn_grc.business_user]. The minimum role for the **sn_compliance.user** is GRC User [sn_grc._user].

For more information on the access control limitations to remediation tasks, see GRC business user role to control access and track usage of compliance tables.

### About this task

Remediating an issue marks an intention to fix the underlying issue causing the control failure or risk exposure. Accepting an issue marks an intention to create an exception for a known control failure or risk. Controls that are **Accepted** remain in a non-compliant state until the control is reassessed. In this way, the issue can be used to document observations during audits.

### Procedure

1. Open the issue you want to remediate.
2. Click the **Remediation Tasks** tab.

**Note:** You have two options for creating a remediation task:

- Click **Suggested Remediation Tasks** and click **Copy** to use an existing task as a basis for creating this task. A copy of the selected remediation task is created with certain information from that task copied to the new task. You can manually complete the other fields.
- Clicking **New** and manually creating the task.

3. On the form, fill in the fields.

**Remediation task form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Assigned to | Select the user responsible for working this task.<br><br>You can configure a hierarchy of users to access the remediation task. For more information, see User hierarchy access control for issue and remediation task records. |
| Issue | The issue for which this task was created. |
| State | The current state of the task. |
| Priority | Select the priority or sequence this task needs to be resolved, based on its impact and urgency. |
| Watch list | Select users who want to be notified when changes occur. |
| Created/Updated | Displays the date/time when the task was created and updated. |
| Name | Brief description of the task. This will appear in lists of tasks. |
| Description | Enter a complete description of the task. |
| Notes and Comments | |
| Additional comments | As needed, enter any customer-facing comments related to this task. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Work notes | Enter any non-customer-facing notes related to the remediation of the issue. |
| Task Schedule | |
| Planned duration | Estimated amount of work time. Calculated using the **Planned start date** and **Planned end date**. |
| Planned start date | Date and time that work on the task is expected to begin. |
| Planned end date | Date and time that work on the task is expected to end. |
| Actual duration | Amount of actual work time. Calculated using the **Actual start date** and **Actual end date**. |
| Actual start date | Time when work began on this task. |
| Actual end date | Time when work on this task was completed. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |

4. Click **Submit**.

## Manage the UCF integration

Network Frontiers Unified Compliance Framework (UCF) integrates with your ServiceNow instance through an authentication process that validates your subscription. On the UCF Configuration form, you select the type of authentication, and then enter a UCF-provided API key or a ServiceNow – provided Oauth2 client and secret.

**Important:** Introduced in Kingston, UCF integration using the ServiceNow-provided Oauth client and the UCF Common Controls Hub is still supported; however, it is no longer the recommended method for integrating your instance with UCF. The preferred method is to configure the UCF integration using a UCF-supplied API key (see link below).

### Activate Compliance UCF

The GRC: Compliance UCF (com.sn_comp_ucf) plugin is available as a separate subscription.

**Before you begin**
Role required: admin

**About this task**
This plugin includes demo data and activates related plugins if they are not already active.

**Procedure**

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the plugin using the filter criteria and search bar.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel.

3. Select **Install**, and then in the Activate Plugin dialog box, select **Activate**.

> **Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: `Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.`

### What to do next

Configure the source of your control library using an API key supplied by UCF (this is the recommended method) or using the UCF Common Controls Hub, which you can purchase as a subscription from the ServiceNow Store. For more information, see Common Controls Hub or Unified Compliance Framework.

### Configure the UCF integration using a UCF-supplied API key

UCF integrates with your ServiceNow instance through an authentication process which validates your subscription.

### Before you begin

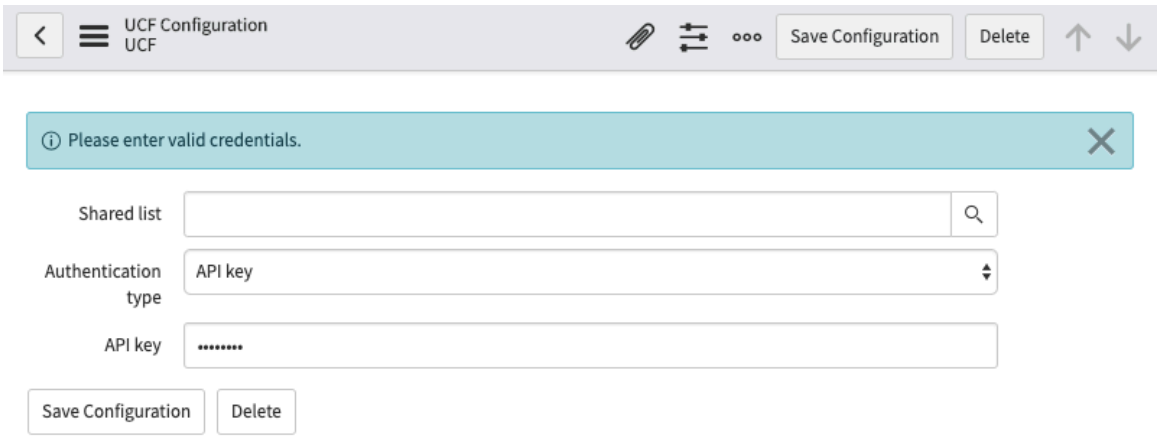
Role required: admin

### About this task

Prior to configuring the UCF integration, you need a UCF basic subscription and use the API Key Manager in your account to acquire an API key from UCF. You must also define shared lists of UCF authority documents in your account.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Unified Compliance Integration**.
2. Click the UCF configuration.




3. On the form, fill in the fields.

#### UCF Configuration

| Field | Description |
|---|---|
| Shared List | Select the shared list from your UCF account. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Authentication type | Select **API Key**. |
| API Key | Enter the API key you acquired from your UCF account. |

4. Click **Save Configuration**.

### Configure the UCF integration using the UCF Common Controls Hub

Compliance administrators can download content from Network Frontiers Unified Compliance Framework (UCF) to use as GRC authority documents, citations, controls, and control objectives.

#### Before you begin

Role required: sn_comp_ucf.admin and oauth_admin
The documents can be updated on pre-defined intervals. You must have a UCF Common Controls Hub account to create shared lists and import them into the ServiceNow® instance. API access is required to download UCF content from the UCF-CCH.

**Note:** Please take note of the following guidelines before configuring the UCF integration using the UCF Common Controls Hub

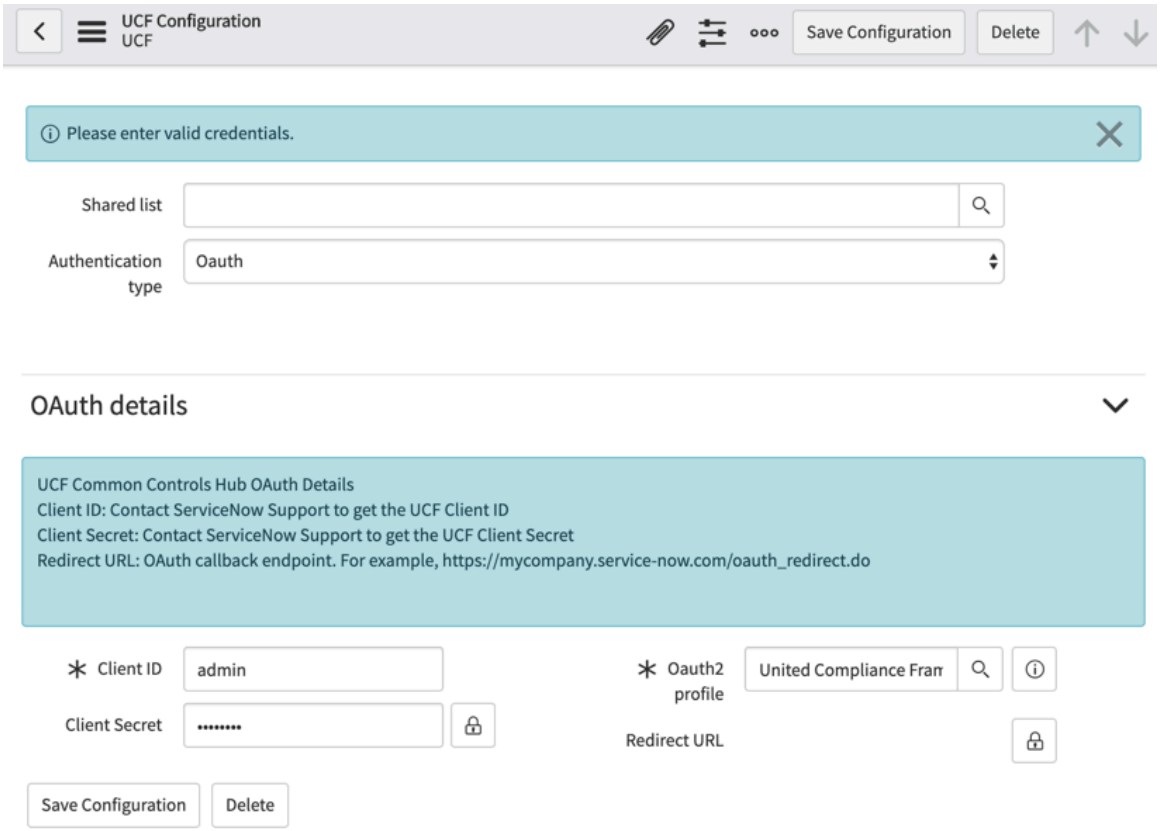
- Only the UCF Oauth administrator has access to the system Oauth tables. You must grant the UCF Oauth administrator role to the GRC UCF administrator, so the UCF administrator can set up UCF configuration page.
- UCF integration requires that GRC is configured and users must be a Common Controls Hub administrator.
- The configuration page for the global domain is loaded by default. If you are using Domain Separation, delete the default configuration page, and create one specific to your domain.

#### About this task

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Unified Compliance Integration**.
2. Click the UCF configuration.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**3.** On the form, fill in the fields.

### UCF Configuration

| Field | Description |
|---|---|
| Shared List | The shared list to be imported.<br>**Note:** Shared lists appear for subscription authentication. |
| Authentication type | Select **Oauth**. |
| **OAuth details** | |
| Client ID | Enter the Client ID or UCF OAuth Client ID provided by Customer Service and Support. See Create a Now Support Case for UCF-CCH account integration information for information.<br>**Note:** Configuration information is specific to the ServiceNow® instance. Be sure to enter accurate information for any test, development, or production instances you are using. Do not include spaces in the entry. |
| Client Secret | Enter a Client Secret to be used by the OAuth Client to authenticate to the Authorization Server. The Client Secret must be sufficiently random to not be guessable. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Oauth2 profile | Enter the OAuth2 profile to use for downloading. The default is the United Compliance Framework Default Profile that is installed with the UCF plugin. This field doesn't typically need to be changed. |
| Redirect URL | Enter the Redirect URL, provided by Customer Service and Support. For example, `https://mycompany.service-now.com/oauth_redirect.do` |

4. Right-click the form header and click **Save**.
5. In the UCF Integration dialog that appears, click **Request New Token**.

> **Note:** For initial configuration, a user with an UCF administrator account performs this setp and the next step.

6. Enter your Common Controls Hub credentials to log in.
7. In the application authorization message that displays, click **Authorize**.
8. Select a shared list and click **Save Configuration**.

### What to do next

If UCF introduces new fields and content, administrators can use staging tables and transform maps to accommodate those changes to UCF data formats. This is an advanced configuration and not required. The following import sets and tables can be configured to customize the UCF download logic.

**Staging table [extends from import set row table: import_set_row] used for UCF integration**

| Staging table | Description |
|---|---|
| UCF Authority Document [sn_comp_ucf_authority_document] | The UCF Authority Document staging table is used to store authority documents that are downloaded from the UCF Common Controls Hub |
| UCF Citation [sn_comp_ucf_citation] | The UCF Citation staging table is used to store citations that are downloaded from the UCF Common Controls Hub |
| UCF Control [sn_comp_ucf_control] | The UCF Control staging table is used to store controls that are downloaded from the UCF Common Controls Hub |
| UCF Citation to Control [sn_comp_ucf_m2m_control_citation] | The UCF Citation to Control staging table is used to store citation to controls that are downloaded from the UCF Common Controls Hub |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Transform maps used for UCF integration**

| Transform maps | Description |
|---|---|
| Default Authority document transform | Transforms data from the UCF Authority document staging table into the Authority Document table |
| Default Citation Transform | Transforms data from the UCF Citation staging table into the Citation table |
| Default Control transform | Transforms data from the UCF Control staging table into the Control Objective table |
| Control to Citation transform map | Transforms data from the UCF Citation to Control table into the Control Objective to Citation table |

### Use UCF Common Controls Hub to manage compliance frameworks

Compliance administrators can download content from Network Frontiers Unified Compliance Framework (UCF) to use as GRC authority documents, citations, controls, and control objectives. The documents can be updated on pre-defined intervals. You must have a UCF Common Controls Hub account to create shared lists and import them into the ServiceNow® instance.

If your organization wants to use UCF Common Controls Hub as the source for your controls library, you can purchase a subscription from the ServiceNow Store or see Common Controls Hub. For more information, see Unified Compliance Framework.

**Note:** The previous arrangement for free access to UCF content inclusive of your GRC license ended November 30, 2018. All customers must purchase a subscription from Unified Compliance directly.

**Warning:** All data imported from UCF Authority Documents is read-only and must be protected. Do not customize the authority documents, citations, or control objectives on any UCF fields transformed into GRC tables.

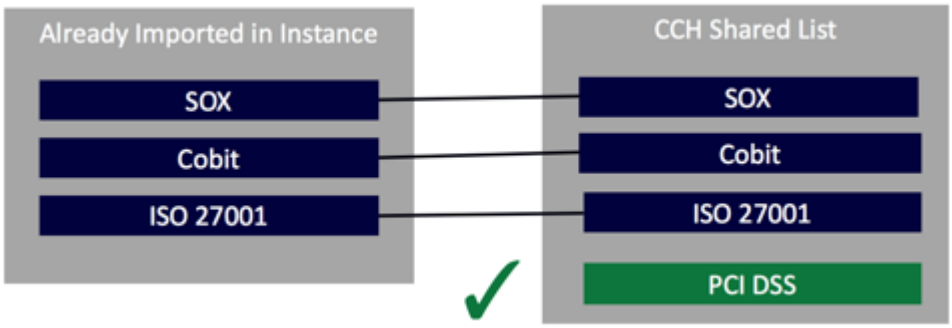
1. Sign up for a UCF CCH account and customize your basic subscription to include API Access.
2. Activate Compliance UCF.
3. Create a Now Support Case for UCF-CCH account integration information.
4. Configure the UCF integration using the UCF Common Controls Hub.
5. Download a UCF shared list.

## Import authority document using single shared list

Every authority document already imported into the ServiceNow® instance must be in any shared list you wish to import from the UCF CCH. This prevents inconsistencies between what is in the UCF CCH (which may have changed) and what you've already imported.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Shared list import successful**




**Shared list import unsuccessful**




An error is rendered since SOX is not being reimported within this Shared List.

## Import authority documents using multiple shared lists

If you need to import more than 100 authority documents then you must import them into multiple shared lists, as there is a limitation that a shared list can contain only 100 authority documents. You can create multiple shared list (SL), for example SL1 to import 100 authority documents and SL2 for the rest of the authority documents. Group similar authority documents as one group when you import the authority documents into multiple shared list, so that there is no dependency of the documents between the multiple shared list.

To support multiple shared list, the system property *sn_comp_ucf.deactivate_deprecated_docs* that is by default **true**, must be set to **false**.

- If the system property is set to true, then the existing validation is done to check if the authority documents imported are already imported in the ServiceNow instance.
- If the system property is set to false, then the imported authority documents are not validated at all.

Set the property as false and import the UCF content in multiple shared list. If the authority documents, citations, and control objectives that are imported in the shared list are deprecated, then such documents will not be deactivated in the ServiceNow instance. Instead, the user must manually validate the documents and the links between the citation and control objectives. An email is sent with the links to the mapping between the citation and control objectives.

## UCF and GRC terminology differences

Authority documents in the UCF content are organized and mapped to their proper citations, which in turn are mapped to a common set of controls. The terminology between UCF and the GRC applications differs slightly as explained in the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Terminology differences

| UCF | GRC application |
|---|---|
| Authority Document | Authority Document |
| Citation | Citation |
| Control | Control Objective |

## Create a Now Support Case for UCF-CCH account integration information

After establishing your UCF CCH account, use the Now Support Service Portal to initiate the account integration process.

### Before you begin

Sign up for a UCF CCH account and customize your basic subscription to include API Access. A user with the UCF administrator role must log into the CCH account and generate the API key.

**Note:** The previous arrangement for free access to UCF content inclusive of your GRC license ended November 30, 2018. All customers must purchase a subscription from Unified Compliance directly.

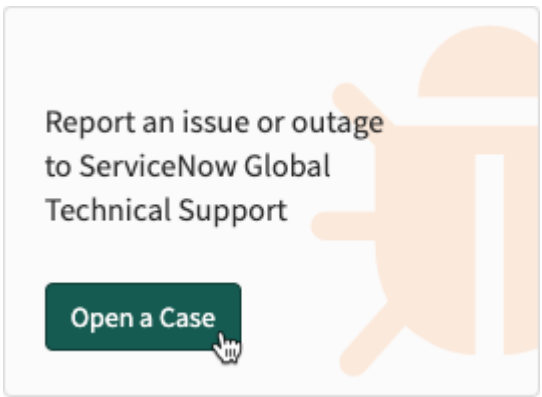
Role required: admin

### Procedure

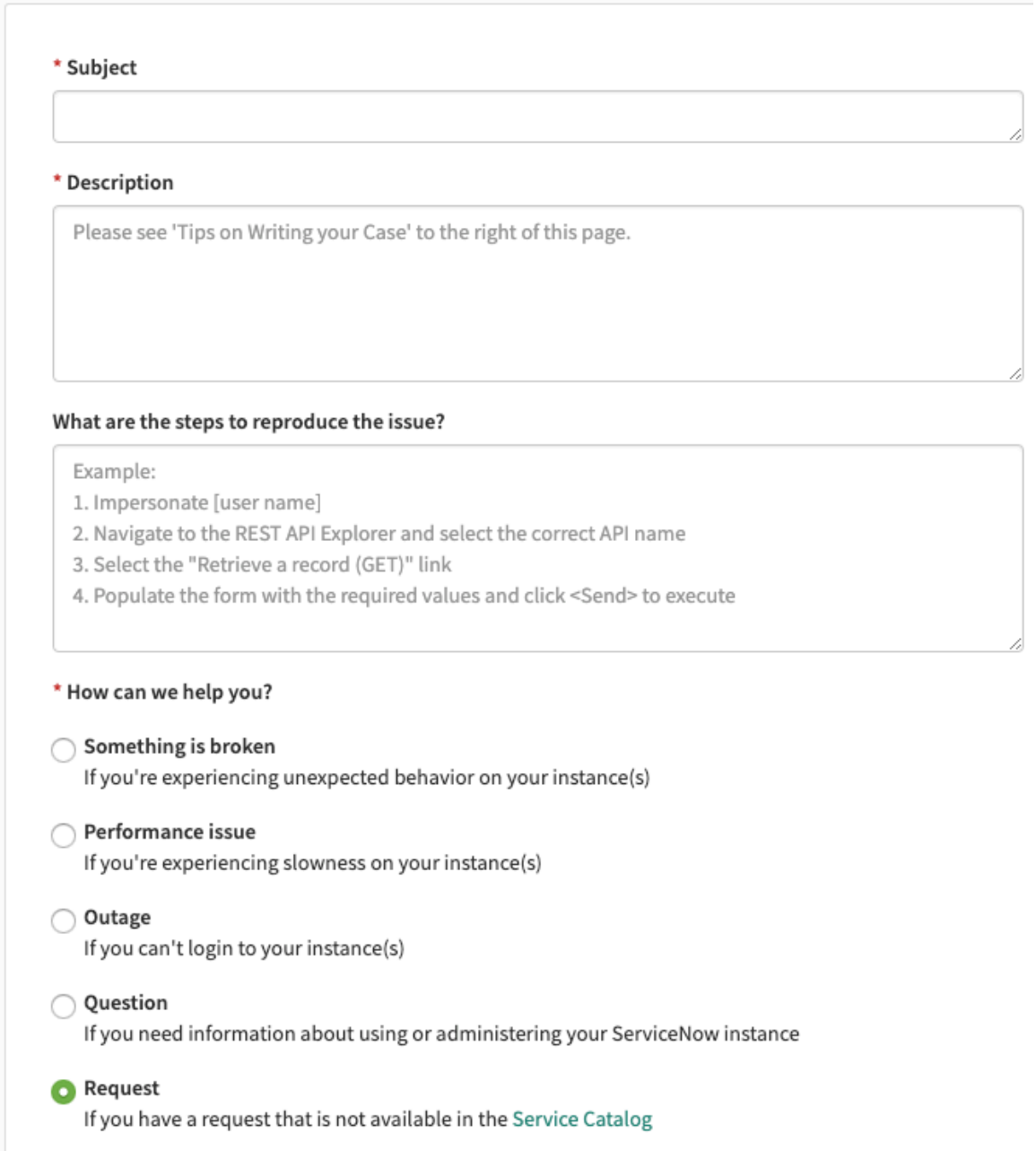
1. After activating the Compliance UCF plugin, sign in to the Hi Service Portal.
2. Click **Get Help**.



3. Click **Open a Case**.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**4.** Fill out the **Create Case** form.

| Field | Description |
|---|---|
| Subject | A brief description of the case. |
| Description | Describe the issue and provide the following information:<br>◦ Enter `I have activated the new GRC: Compliance UCF (com.sn_comp_ucf) plugin. I have already subscribed to the UCF CCH. I am requesting that you provide me with the necessary OAuth information to complete the integration.`<br>◦ Include your company name and company account number.<br>◦ Include the requester's name, business email address, and phone number. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** By providing your company and requester contact information, you authorize ServiceNow® customer service to contact and share that information with Network Frontiers, a third party, to complete your UCF CCH account enrollment. |
| How can we help you? | Click **Request**. |
| Attachments (screenshots, logs, etc.) | Attach screenshots, as necessary. |
| Which of your instances are affected? | Enter your company's GRC instance. |
| What is the impact? | Select your answer. |

5. Click **Submit**.
   Customer Service and Support initiates the OAuth integration process and contacts the requester with the integration information.

### Download a UCF shared list

In order for compliance managers to download UCF authority documents from the UCF CCH, the list must be marked as Shared. When updating Authority Documents or adding new ones, you must update all your authority documents to ensure that the common controls framework remains in sync with the authority documents you are using.

#### Before you begin

Role required: sn_compliance_admin or sn_compliance_manager

**Note:** The current design of UCF supports the downloading of mandated and implied controls. The downloading of implementation controls is not supported. See the Unified Compliance Documentation How do I distribute an authority document list to other accounts? .

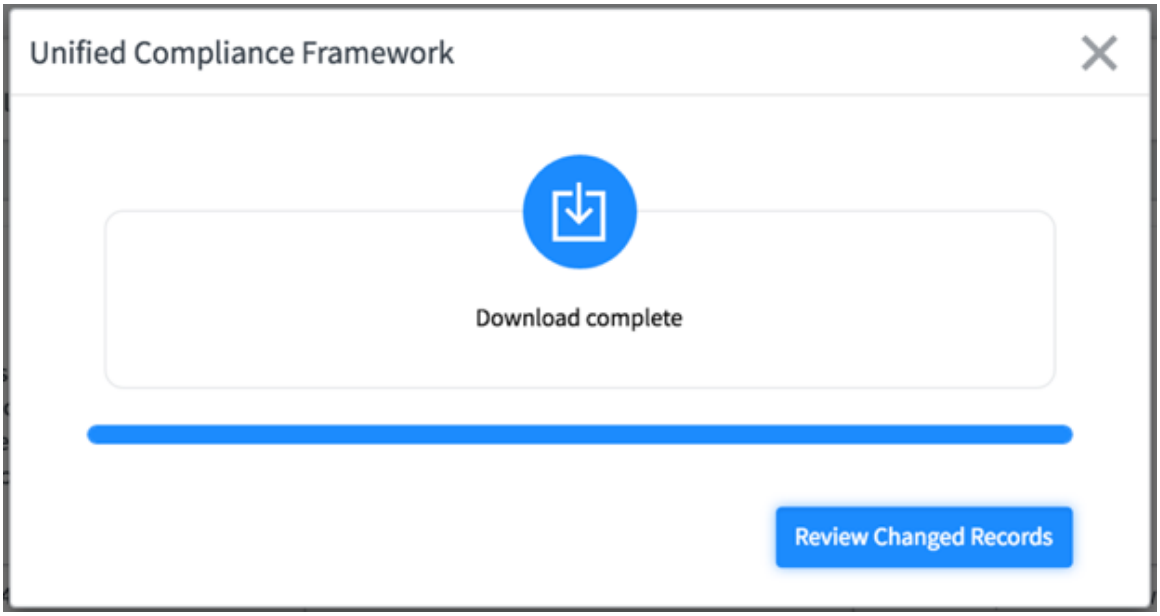
All data imported from UCF Authority Documents is read-only and must be protected. Do not customize the authority documents, citations, or control objectives on any UCF fields on the GRC tables.

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Unified Compliance Integration**.
2. Click the **UCF** configuration.
3. Configure the UCF integration using the UCF Common Controls Hub, if necessary.
4. Click **Import Shared List**.

   A progress bar shows the progress of downloading and importing the documents.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




You may encounter any of the following errors:

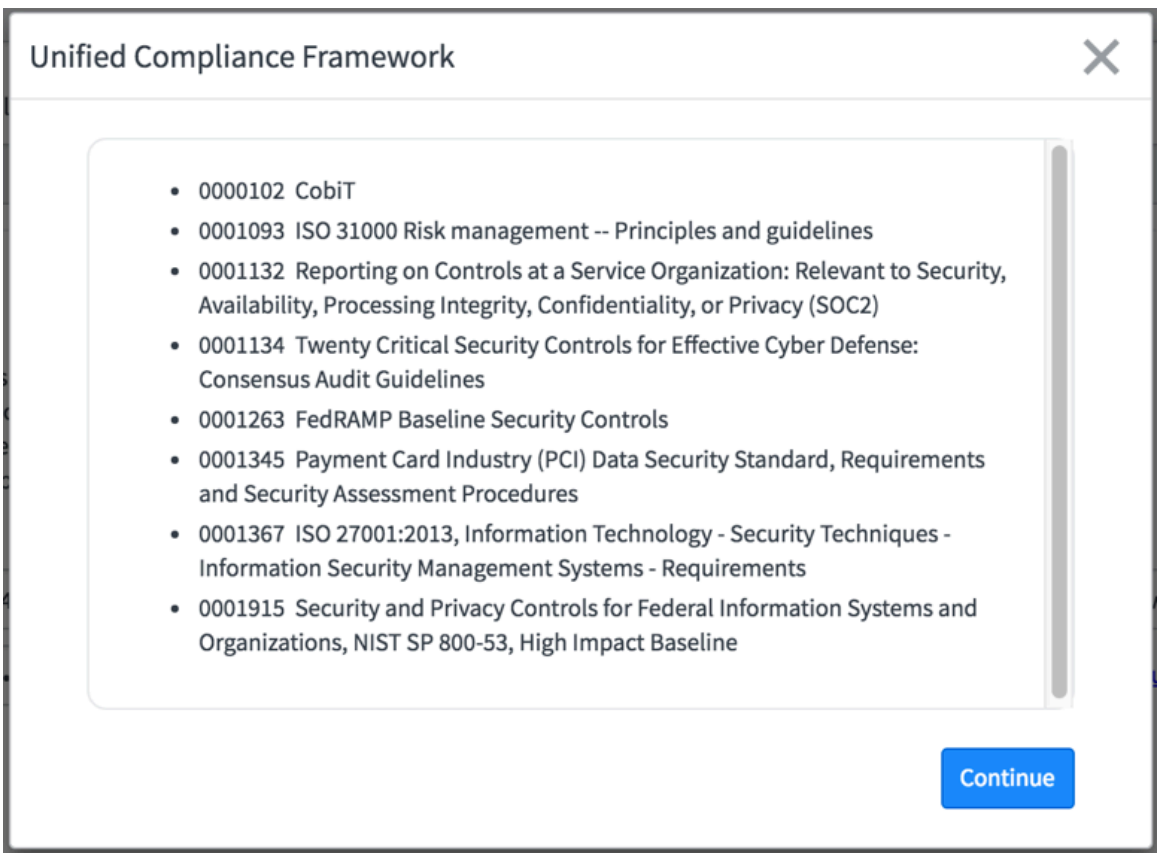
### UCF Shared List Errors

| Error | Explanation | Resolve |
|---|---|---|
| Error encountered while downloading UCF content. Try again or contact your system administrator for further assistance. | If the internet connection is lost for any reason, this message appears. | Click **Import Shared List** to download again. |
| Error encountered while downloading UCF content. Try again or contact your system administrator | This message may also indicate that the authority documents are part of an existing shared list or a possibility of a UCF import error. It suggests that you review the validity of the authority | Starting with Policy and Compliance Management version 12.0.4, your UCF Administrator receives an email with links to any invalid records.<br>**a.** Click a link in the mail and fix the record(s) listed.<br>**b.** Repeat for other invalid records, if they appear in the email.<br>**c.** Click **Import Shared List** to download again. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Error | Explanation | Resolve |
|---|---|---|
| for further assistance. | documents, citations, control objectives, and the links to the mapping of citation and control objectives. | **Note:**<br>A system property called *sn_comp_ucf.deactivate_deprecated_docs* controls whether an email notification is sent when invalid or deprecated records are encountered during a shared list import. The property defaults to true. Set the property as false if you are downloading UCF content in multiple shared list. When the property is set as false the documents are not deprecated but an email is sent. |
| The selected Shared List does not match the existing Authority Document list. Select a different Shared List or update the existing Shared List. | If the selected UCF Shared List that you are downloading does not include all the authority documents you have already downloaded, this message appears. | **a.** Return to the CCH and verify that the Shared List you are trying to download includes all the Authority Documents from the original import to your instance.<br>**b.** Click **Import Shared List** to download again. |

5. Click **Review Changed Records** to review the list of changed records.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Authority documents in the UCF content are organized and mapped to their proper citations, which in turn are mapped to a common set of controls. The terminology between UCF and the GRC applications differs slightly as explained in the following table.

**Terminology differences**

| UCF | ServiceNow GRC application |
|---|---|
| Authority Document | Authority Document |
| Citation | Citation |
| Control | Control objective |

## Manage controls

Controls are specific implementations of a control objective. Retired controls do not appear in the list. Before defining controls, take time to rationalize, consolidate, and define the important controls in your organization.

## Rationalize your controls

If you upload all your controls in bulk, you are missing the opportunity to refine and streamline your controls set. As your business changes, and your IT data, processes, and technology improve, replace outdated controls and procedures when you implement your GRC application. Consider the following:

- How does this control affect my business objective?
- Is this control actually preventing or detecting risk?
- Is there a different control you can place that better protects your business?
- Is there a control you can put in place that reduces process overhead and improves IT performance while also mitigating risk?
- Can a complicated control be replaced with a simpler more effective control?

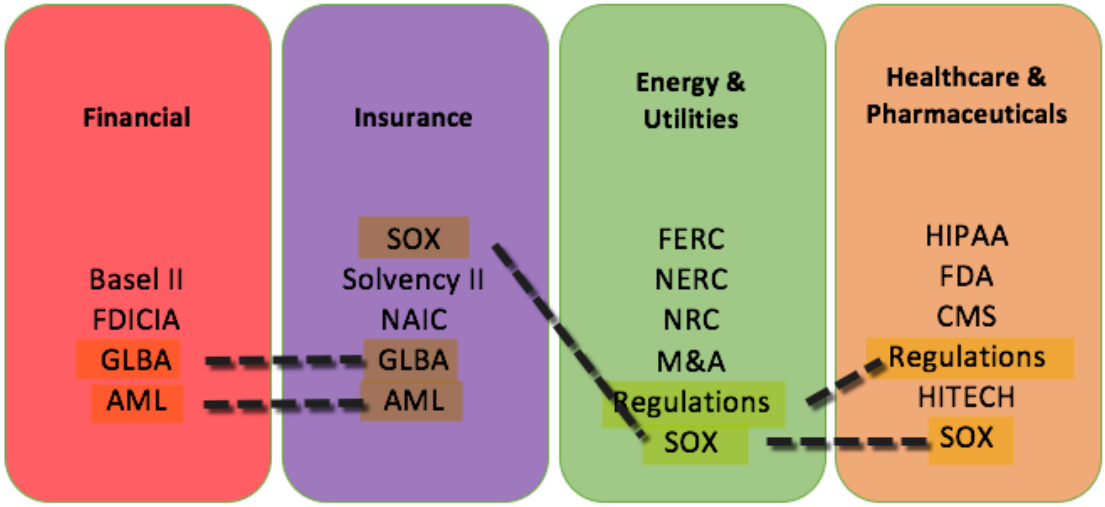
**Note:** When you define controls manually or when you import them from the Unified Compliance Framework (UCF), an entity is associated with the controls. It is a mandatory field on the Control form. If, however, you import controls from a source other than the UCF, you may encounter controls that do not have associated entities. It is important that you return to the Control form and add an entity to the control. Missing entities can cause unreliable results in calculations. Also, if you encounter a control with an entity that has been disabled, the control should be retired.

## Consolidate your controls

Look for opportunities to consolidate controls. Look for common, repeated controls across multiple regulatory authorities of frameworks (for example, SOX and GLBA and AML). Avoid operating a single control multiple times for each regulation, by cross-mapping controls and eliminating the redundant ones. This process establishes a single consolidated set of controls = control framework, performing and preserving the cross mapping of controls is critical for audits.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Industry regulations and requirements overlap**




## Define controls and business rules

The business rules you define up front, establish the GRC configuration settings later. Be prepared to:

- Identify controls and control owners
- Define control tests and expected results
- Establish test and control frequencies
- Identify risks: impact and likelihood
- Prepare attestations, assessments, questionnaires, and required evidence
- Compose likely use-cases (who needs to interact with or view the contents of the GRC system and for what purposes)
- Map authoritative sources to policies, to procedures, to controls, and to risks

### Create a control

Controls are automatically generated when you associate a policy with an entity type or an entity type with a control objective. A control is created for each entity listed in the entity type for the control objective. Controls can also be manually created.

**Before you begin**
Role required: sn_compliance.admin or sn_compliance.manager

**Procedure**

1. Navigate to **All** > **Policy and Compliance** > **Controls** > **All Controls**.
2. Click **New**.
3. On the form, fill in the fields.

**Control form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the control. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Entity | Related entity.<br><br>**Note:** If you change the state of the entity to Active from Retired state, then the manually created control on the entity also moves to the Draft state. |
| Inherit from control objective | Option to indicate whether the control is created through item generation process. For more information, see Multiple controls for a unique entity–control objective combination. |
| Control Objective | Related control objective. |
| Owning group | Group that owns the policy. |
| Owner | User that owns the policy.<br><br>**Note:** The owner is always added as a respondent. The control owner that you select belongs to the owning group. |
| Key control | Indicator that the control is a key control. |
| Weighting | Value used to calculate the control score effectiveness. Based on the control weighting, in the control score effectiveness value is calculated |
| Status | Control status. Possible choices are:<br><br>◦ **Compliant**<br>◦ **Non-compliant**<br>◦ **Not applicable** |
| State | Control state. Possible choices are:<br>◦ **Draft** In this state, all compliance users can modify the control. Only available when creating a one-off control. One-off controls are possible but not recommended.<br>◦ **Attest** When the control is created from a control objective, controls are in this state.<br><br>**Note:** When a control is set back to draft, the attestation is canceled.<br><br>◦ **Review** Controls are automatically moved to review from the attestation phase.<br>◦ **Monitor** In this state, all compliance managers can move the control from review to monitor. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ **Retired** Compliance managers or administrators can move a control from Monitor to Retired.<br><br>**Note:** When a control is retired:<br>▪ Associated indicators do not run<br>▪ Associated attestations are canceled<br>▪ Changes to associated control objectives do not update the control |
| Enforcement | List of options:<br><br>◦ Mandated<br>◦ Voluntary |
| Category | List of options:<br><br>◦ Acquisition or sale of facilities, technology, and services<br>◦ Audits and risk management<br>◦ Compliance and Governance Manual of Style<br>◦ Human Resources management<br>◦ Leadership and high-level objectives<br>◦ Monitoring and measurement<br>◦ Operational management<br>◦ Physical and environmental protection<br>◦ Privacy protection for information and data<br>◦ Records management<br>◦ System hardening through configuration management<br>◦ Systems continuity<br>◦ Systems design, build, and implementation<br>◦ Technical security<br>◦ Third Party and supply chain oversight<br>◦ Root<br>◦ Deprecated |
| Type | List of options:<br><br>◦ Acquisition/Sale of Assets or Services<br>◦ Actionable Reports or Measurements<br>◦ Audits and Risk Management<br>◦ Behavior<br>◦ Business Processes<br>◦ Communicate<br>◦ Configuration |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Data and Information Management<br>◦ Duplicate<br>◦ Establish Roles<br>◦ Establish/Maintain Documentation<br>◦ Human Resources Management<br>◦ Investigate<br>◦ IT Impact Zone<br>◦ Log Management<br>◦ Maintenance<br>◦ Monitor and Evaluate Occurrences<br>◦ Physical and Environmental Protection<br>◦ Process or Activity<br>◦ Records Management<br>◦ Systems Continuity<br>◦ Systems Design, Build, and Implementation<br>◦ Technical Security<br>◦ Testing<br>◦ Training |
| Classification | List of options:<br><br>◦ Preventive<br>◦ Corrective<br>◦ Detective<br>◦ IT Impact Zone |
| Frequency | List of options:<br><br>◦ Event Driven<br>◦ Daily<br>◦ Weekly<br>◦ Monthly<br>◦ Quarterly<br>◦ Semi-Annually<br>◦ Annually<br><br>**Note:** For information on the difference between the**Frequency** field for a control and the**Attestation Frequency** field in an entity, see KB0694607. |
| Description | Description of the control. |
| Additional Information | Additional information about the control. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Assignment | |
| Owning group | Group that owns the control. |
| Owner | User that owns the control. |
| Attestation | |
| Attestation | Select from a list of options.<br>◦ Other attestation types can be configured.<br>◦ If this field is populated, then the **Attestation Respondents** field automatically becomes mandatory, and the owner is made the respondent.<br>**Note:** If the user changes the attestation type in the control objective, all the related controls are changed also. |
| Attestation respondents | ◦ Users assigned to the attestation of this control.<br>◦ Only a user with the sn_grc.user role can be added as a respondent.<br>**Note:** When both the **Attestation** and **Attestation respondents** fields are set, attestations are created when you click **Attest**. |
| Activity Journal | |
| Additional comments | Public information about the control. |

4. Click **Submit**.

### What to do next

After you create a control, you can convert the control to a common control and add reliant entities and reliant entity types to it. For more information, see Testing common control and implementing results on multiple reliant entities.

#### Follow a control

Connect integrates with Policy and Compliance Management providing an overlay to the standard interface, allowing users to participate in conversations while they work and collaborate on the control record.

### Before you begin

Role required: sn_compliance.user or sn_compliance.reader
For more information about Connect, see Connect.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Controls** > **All Controls**.
2. Open the control record.
3. Click **Follow** > **Following** and select one of the options from the drop-down.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Action |
| --- | --- |
| To add the Connect sidebar | Click **Open Connect mini**. |
| To add the Connect full-screen view | Click **Open Connect Full**. |

### Attest a control

Attestations are surveys that gather evidence to prove that a control is implemented. If the control attestation and respondents fields are selected, when the control moves from the **Draft** state to the **Attest** state, a notification is sent to the attestation respondents.

#### Before you begin

Role required: sn_grc.user
Users can create multiple attestation types and set their control objectives to different attestations. A sample attestation called **GRC Attestation** is also provided as the default attestation.

#### About this task

When controls are attested, a new questionnaire is created. As a result, attestations do not appear in the **Self-Service** > **My assessments & surveys** module. Hundreds of GRC assessment records could be generated at once and should be separated from other assessments in a separate list view.

#### Procedure

1. Navigate to **Policy and Compliance** > **Controls** > **My Attestations**.
2. Open the attestation and review the details.

| Option | Description |
| --- | --- |
| If you are unable to answer the questions | **a.** Reassign the attestation to another user in the **Assigned to** field.<br>**b.** Click **Update** and close the record.<br>**Note:** Only a user with the sn_grc.user role can be re-assigned the attestation.<br>The list of attestations refreshes when you re-assign an attestation to another user. |
| If you are able to answer the questions | **a.** Click **Take attestation**.<br>**b.** Answer the questions and attach information, as required.<br>**c.** Click **Submit**.<br>The list of attestations refreshes when you close the **Take Assessment** pop-up window. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Multiple controls for a unique entity–control objective combination

You can create multiple controls for a unique combination of an entity and a control objective to get granular control information.

For an organization that handles multiple products, operational lines, and practices, having a single control for an entity and a control objective combination is ineffective. Multiple levels of control objectives, controlled and managed centrally helps to get the granular control information.

The benefits of creating multiple controls for the same entity and control objective combinations are:

- You can create high-level control objectives and more granular controls.
- The control owner, compliance manager, and compliance user can manage the compliance library more efficiently.

You can create multiple controls for the same combination of entity and control objective by enabling the **Inherit from control objective** option in the Control form. Controls can be created either through item generation process or, by default, inherited from the control objective. Such controls have a unique name as they are unique to the entity–control objective combination. By default, only one control can be inherited from the control objective. However, if you want to create multiple controls for the same combination of entity and control objective you have to do it manually and the name of the control must be unique.

When you select the **Inherit from control objective** option in the Control form, the control automatically inherits the name and description of the control objective. However, when the option is not selected, then you must enter the name of the control manually.

## Manage control attestations

Attestations are surveys that gather evidence to prove that a control is implemented. The attestation designer provides a single interface that users can use to create, and edit attestations, as well as change scoring parameters. The question bank offers a library of questions for various categories, so you do not have to build each questionnaire from scratch.

Users can create multiple attestation types and set their control objectives to different attestations. A sample attestation called **GRC Attestation** is also provided as the default attestation, which is composed of the following simple questions:

By default, **GRC Attestation** is used for controls and provides the following assessment questions:

- Is this control implemented?
- Attach evidence
- Explain

**My Attestations** is in the **Controls** section of the Policy and Compliance application and contains active attestations for which you are the respondent. The attestations appear in a list with a single attestation record per control.

**My Grouped Attestations** contains attestations that you have grouped to eliminate the task of providing repetitive responses for similar assessments.

**All Attestations** is contained in the **Controls** section of the Policy and Compliance application and contains all active attestations.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Compliance managers can create attestation types containing different types of questions to fit their needs. See Create a control attestation using the Attestation Designer.

Compliance managers can create a new set of questions for each control objective. The Question Bank offers a library of questions for various categories, so you do not have to build each questionnaire from scratch. See Create an attestation type.

## Attestation Designer

The attestation designer provides a single interface that users can use to create, and edit attestations, as well as change scoring parameters.

All attestation records are stored in assessment tables and displayed in Attestation views of those tables.

### Create a control attestation using the Attestation Designer

Use the Attestation Designer to create and edit metric types. Use different metric types for different controls. Select multiple respondents for an attestation, as well as change scoring parameters.

#### Before you begin

Role required: sn_compliance.attest_creator, sn_compliance.manager, sn_compliance.administrator

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Attestation Types**.
2. Click **Attestation Designer**.
   The designer contains the following elements:

| Element | Description |
|---|---|
| Controls | Supported question data types are available in the Controls palette. Drag a control onto the designer canvas to create a question of that type. |
| Questions | A library of questions for various categories, so you do not have to build each questionnaire from scratch. |
| Categories | New assessment opens in the **Design** view. The questionnaire **Name** field appears above the first category in the canvas. A blank question field appears in the category container. |

3. Enter a name in the **Name** field.
4. Drag a control onto the designer canvas to create a question of that type.

#### Question controls

| Data type | Description | Scored |
|---|---|---|
| Attachment | Question with a Manage Attachments icon that allows users to attach one or more files. | N |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Data type | Description | Scored |
|---|---|---|
| Boolean | Question with a check box or a **Yes/No** list for user responses. | Y |
| Choice | List of predefined options. For more information, see the definition for **Choices**. | Y |
| Date | Date field. | N |
| Date/Time | Date and time field. | N |
| Number | Number field with predefined minimum and maximum values. The default is 1–10. | N |
| Percentage | Percentage field with a prescribed range. | N |
| Scale | Predefined Likert scale. Answer options appear as radio buttons. | Y |
| Numeric Scale | Selectable number scale. The default is 1–5. Answer options appear as radio buttons. | Y |
| String | Single or multi-line text field. | N |
| Template | Choice list of templates that provide a predefined scale of options.<br>**Note:** It is important to assign a template to every attestation. This allows controls to be created automatically based on control objectives and entity types. | Y |
| Reference | Choice list of fields from a specified reference table. This data type does not support reference qualifiers. | N |

**Note:** Set the correct answer for the metric that you want to be scored. Scored metrics determine the compliance status of the controls.

5. Point to the menu icon in the upper right of the Attestation Designer to select one of the following options.

**Note:** The availability of each option depends on the status of the attestation that is opened in the designer.

| Option | Description |
|---|---|
| New Attestation | Opens a fresh canvas for a new attestation. |
| Load Attestation | Opens a list of existing attestations that you can select and edit. |

Unlike other types of assessments, control attestations do not appear in the **Self-Service** > **My assessments & surveys** module, because many control attestations could be generated at once. Instead, controls attestations are shown as a list in the **Policy and Compliance** > **Controls** > **My Attestations** module and **All Attestations** module.

### What to do next

If you are implementing the Policy and Compliance Management software, return to the Policy and Compliance Management setup checklist and proceed to the next step.

### Create an attestation type

Rather than using the default **GRC attestation** type, the compliance manager can create a new set of questions for each control objective.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_compliance.attestation_creator or sn_compliance.manager or sn_compliance-admin

### Procedure
1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Attestation Types**.
2. Click **New**.
3. On the form, fill in the fields.

**Assessment Metric Type form**

| Field | Description |
|---|---|
| Name | Name of the assessment type. |
| Assessment duration | Length of time allowed from generation to completion of the assessment. |
| Table | Table this assessment applies to. |
| Scale factor | Scale value to use for all assessment results. |
| Condition | Define specifics records from the table. |
| Description | More details about the assessment. |
| State | State of the assessment: **Draft** or **Published** |
| Enforce condition | Option that indicates whether accessible records of this type that do not meet the conditions specified are deleted. |
| Roles | Roles that have access to information about this metric type. |

4. Click **Submit**.

## Consolidate control attestations using the Same Response feature

Policy and Compliance Management and Risk Management offer two methods for consolidating attestations and risk assessments into groups that help eliminate the task of providing repetitive responses for similar assessments. You can provide the same evidence to the grouped assessments or respond to individual assessments in the same user interface.

### Before you begin
Role required: sn_grc.business_user, sn_grc.business_user_lite

### About this task
When you consolidate control attestations using the Same Response feature, you can group attestations that contain a maximum of 1000 questions. When the attestation or risk assessment for the group is taken, all records in the group inherit the answers.

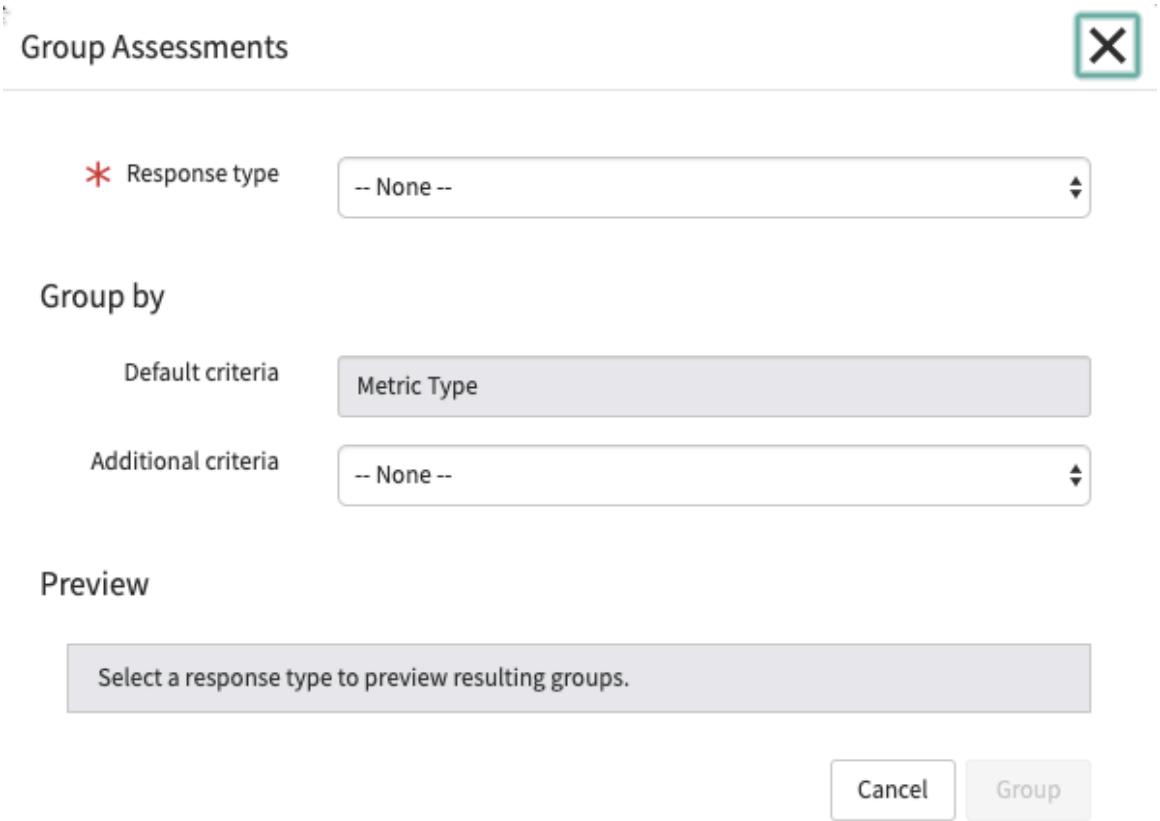
**Note:** To change the 1000-question limit, navigate to **All** > **Policy and Compliance** > **Administration** > **GRC Properties** and modify the **sn_grc.consolidated_questions_limit** property.

If you do not want your users to access to this capability, navigate to **All** > **Policy and Compliance** > **Administration** > **GRC Properties**, and disable the **sn_grc.enable_consolidate_asmt** property.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Controls** > **My Attestations**.
2. Select the attestations you want to group.
3. From the **Actions on selected rows** choice list, click **Group Assessments**.




4. In **Response Type**, select **Provide same response for all assessments**.
5. Fill in the fields, as needed.

| Field | Description |
|---|---|
| Default criteria | This field defaults to **Metric Type**. |
| Additional criteria | You can optionally define additional grouping criteria:<br>◦ Category<br>◦ Control Objective/Risk Statement<br>◦ Entity<br>You can also define additional assessment criteria options if the defaults do not meet your needs. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** Using these grouping schemes makes sense if the grouped attestations contain multiple instances of the selected criteria. For example, if you selected a group of 20 attestations with 10 associated with one entity and the other 10 associated with a different entity, selecting **Entity** in this field causes two separate groups of attestations to be created. If, however, the group consists of 5 attestations associated with one entity and each of the other 15 attestations associated with different entities, only those 5 are grouped and the rest are ignored. |
| Preview | The **Preview** shows the number of attestations to be grouped. Depending on the **Additional criteria** you selected, the Preview may show multiple groups. If you want to see the attestations to be grouped, click the link that shows the number of attestations or risk assessments to be grouped. |

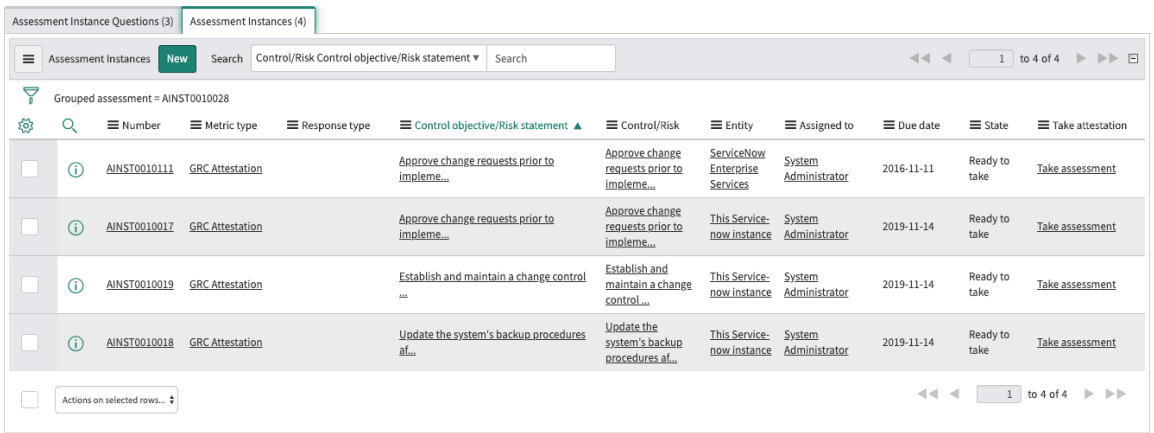
6. When you are satisfied with the attestations or risk assessments to be consolidated, click **Group**.

   A confirmation message displays, along with a link to the attestation group.




**Note:** When attestation groups are created, you can view them by navigating to **Policy and Compliance** > **Controls** > **My Grouped Attestations**. If you open a grouped attestation, you have the option of removing one or more attestations from the group. This is achieved by selecting the ones you want removed, and selecting **Ungroup Assessment** from the **Actions on selected rows** choice list. If you remove attestations from a group to the point where there is only one attestation, the group is removed.

7. When you are ready to take the assessment, click the link in the confirmation message or the attestation number in **My Grouped Attestations**.




8. Click **Take assessment**.
9. Complete the assessment like you would any other, and click **Submit**.
   All attestations in the group inherit the answers you provided and the state of each attestation in the group changes to **Complete**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Consolidate control attestations using the Different Response feature

Policy and Compliance Management and Risk Management offer two methods for consolidating attestations and risk assessments into groups that help eliminate the task of providing repetitive responses for similar assessments. You can provide the same evidence to the grouped assessments or respond to individual assessments in the same user interface.

#### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

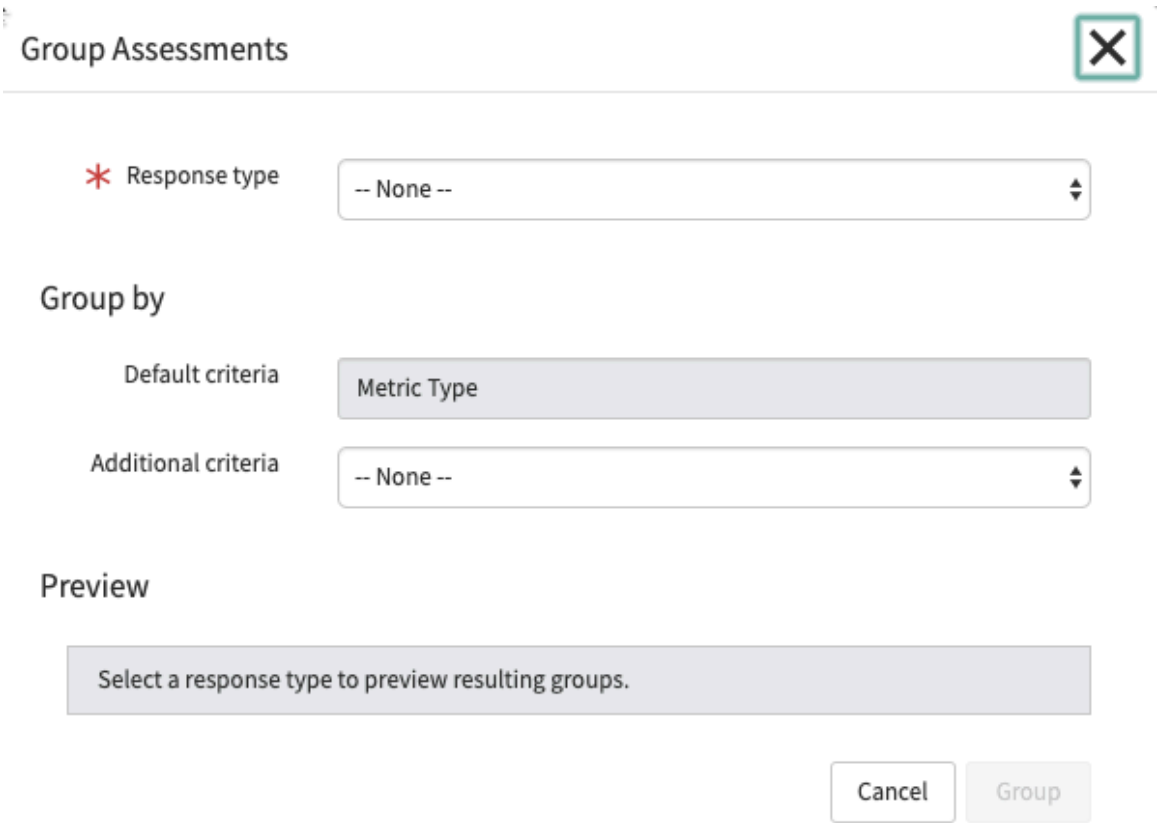
#### About this task

When you consolidate control attestations or risk assessments using the Different Response feature, you can group up attestations or risk assessments that contain a maximum of 150 questions. All of the questions appear in a single UI.

**Note:** To change the 1000-question limit, navigate to **Policy and Compliance** > **Administration** > **GRC Properties** and modify the **sn_grc.grouped_questions_limit** property.

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Controls** > **My Attestations**.
2. Select the attestations you want to group.
3. From the **Actions on selected rows** choice list, click **Group Assessments**.



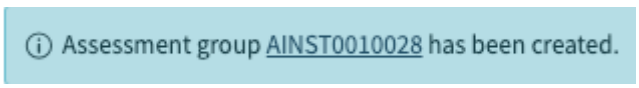

4. In **Response Type**, select **Provide different response for each assessment**.
5. Fill in the fields, as needed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Default criteria | This field defaults to **Metric Type**. |
| Additional criteria | You can optionally define additional grouping criteria:<br>◦ Category<br>◦ Control Objective/Risk Statement<br>◦ Entity<br>You can also define additional assessment criteria options if the defaults do not meet your needs.<br>**Note:** Using these grouping schemes makes sense if the grouped attestations contain multiple instances of the selected criteria. For example, if you selected a group of 20 attestations with 10 associated with one entity and the other 10 associated with a different entity, selecting **Entity** in this field causes two separate groups of attestations to be created. If, however, the group consists of 5 attestations associated with one entity and each of the other 15 attestations associated with different entities, only those 5 are grouped and the rest are ignored. |
| Preview | The **Preview** shows the number of attestations to be grouped. Depending on the **Additional criteria** you selected, the Preview may show multiple groups. If you want to see the attestations to be grouped, click the link that shows the number of attestations or risk assessments to be grouped. |

6. When you are satisfied with the attestations or risk assessments to be consolidated, click **Group**.

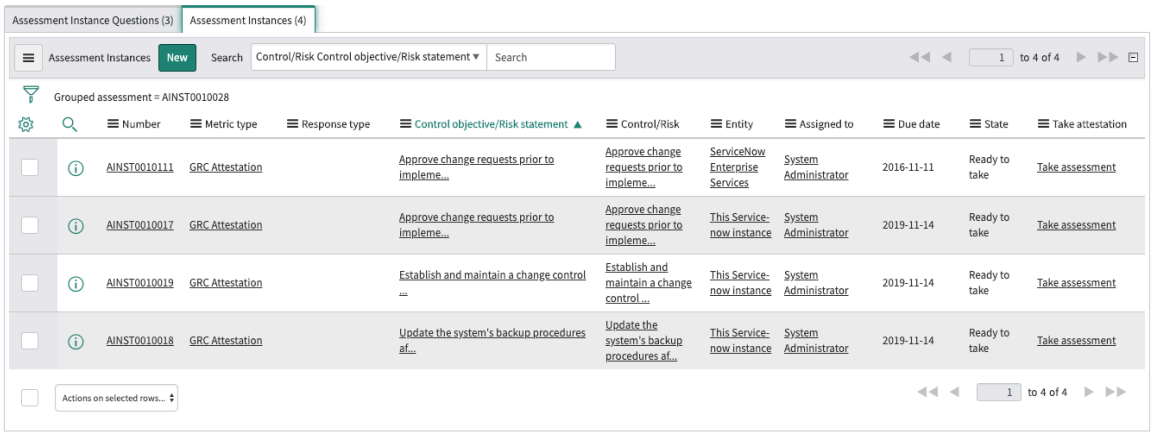
   A confirmation message displays, along with a link to the attestation group.




**Note:** When attestation groups are created, you can view them by navigating to **Policy and Compliance** > **Controls** > **My Grouped Attestations**. If you open a grouped attestation, you have the option of removing one or more attestations from the group. This is achieved by selecting the ones you want removed, and selecting **Ungroup Assessment** from the **Actions on selected rows** choice list. If you remove attestations from a group to the point where there is only one attestation, the group is removed.

7. When you are ready to take the assessment, click the link in the confirmation message or the attestation number in **My Grouped Attestations**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




8. Click **Take assessment**.
   You see questionnaires for all of the selected attestations in the group.
9. Complete the assessment for each of the attestations, and click **Submit**.

## Define assessment grouping criteria

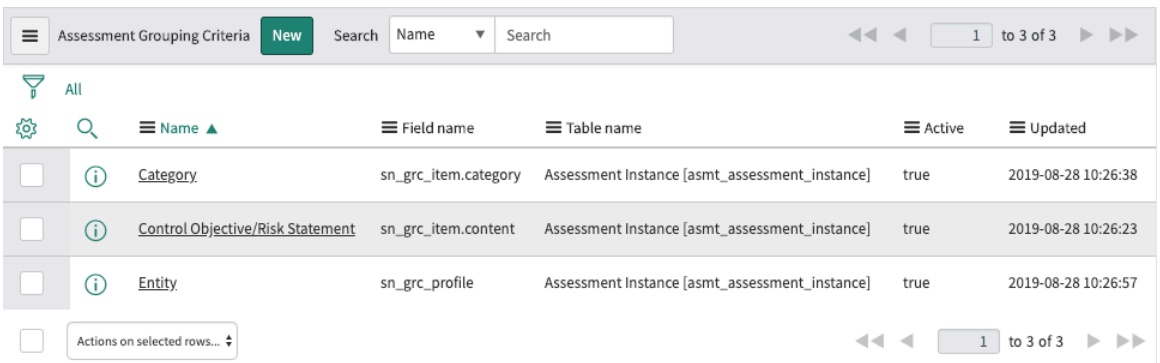
You can optionally define additional grouping criteria if the default criteria does not meet your needs.

### Before you begin

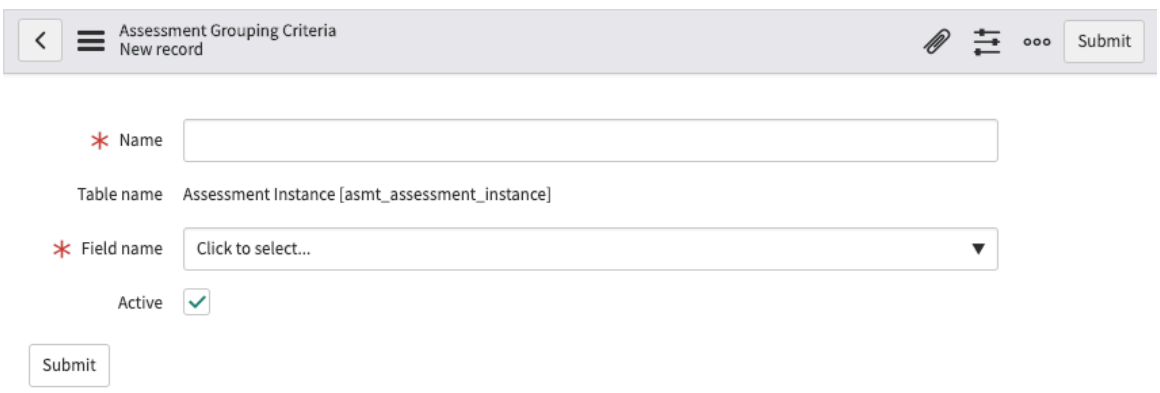
Role required: sn_compliance.admin, sn_compliance.manager

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Assessment Grouping Criteria**.




2. Click **New**.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

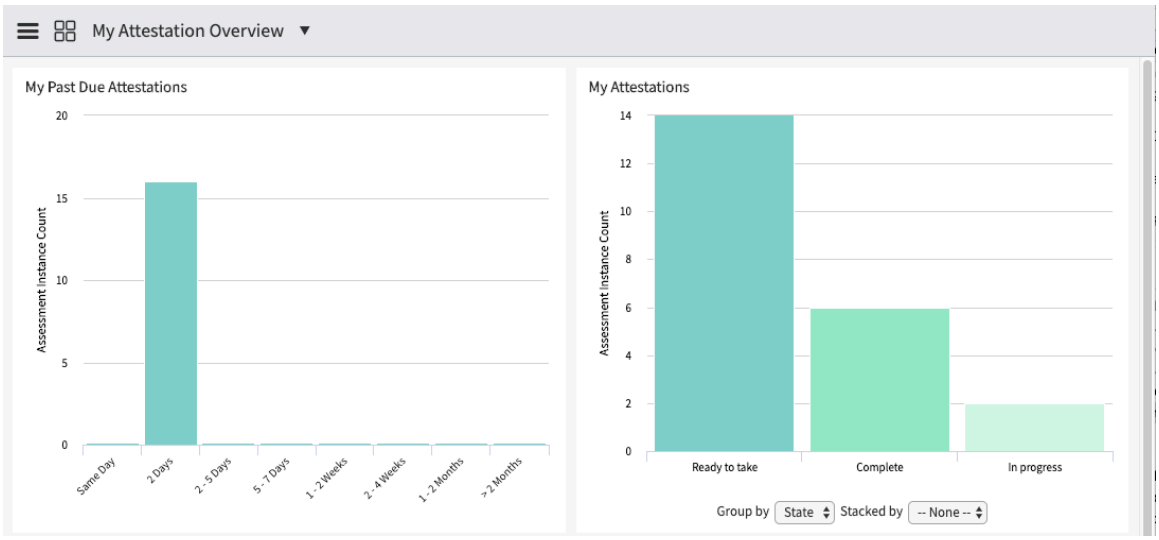
3. On the form, fill in the fields.

| Field | Description |
|---|---|
| Name | Name of the assessment grouping criteria. |
| Field name | Select the field name from the Assessment Instance [asmt_assessment_instance ]table. |
| Active | Select to activate the grouping croteria. |

4. Click **Submit**.

### GRC Attestation Overview dashboard

The GRC Attestation Overview dashboard provides views attestations assigned to you, as well as pending and overdue attestations.




## Reports

The GRC Attestation Overview dashboard contains the following reports:

| Name | Type | Description |
|---|---|---|
| My Past Due Attestations | Column | Total number of past due attestations assigned to you |
| My Attestations | Column | Total number of attestations assigned to you, broken down by state |
| My Pending Attestations | List | A list of the pending attestations assigned to you |

## Manage control indicators

Continuous monitoring involves activities related to identifying and creating key risk and controls indicators. The Compliance Overview is available to compliance administrators and compliance managers, providing an executive view into compliance requirements, overall compliance, and compliance breakdowns.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Supporting information can be collected for indicators through automatic data collection or manual tasks. Indicator results are then used to create issues for controls, update risk scores, and provide supporting information for audit activities and control testing.

Indicators

Indicators collect data to monitor controls and risks, and collect audit evidence. Indicators monitor a single control or risk.

Indicator templates

Indicator templates allow the creation of multiple indicators for similar controls or risks.

## Compliance Overview

**Compliance Overview reports in the base system**

| Name | Visual | Description |
|---|---|---|
| Compliance Requirements | Donut chart | Select a wedge to focus on a specific compliance area. |
| Overall Compliance | Donut chart | Displays the overall compliance of all the control requirements in the system. Selecting a specific wedge in the previous widget brings that area into focus. |
| Entity | Drop down list | Select one or more entities to view and compare their compliance across multiple items. |
| Control State | Check list | Select or clear check boxes to view filter reports by control state. |
| Compliance by Authority Document | Bar Chart | Compare level of compliance depending on the selected entity and/or authority document. |
| Compliance breakdown | Multi-level Pivot | View a breakdown of control compliance by related authority documents and policies. |
| Non Compliant Entities | Column Chart | Count of non-compliant control requirements grouped by entity. |

## Authority Documents

Authority documents define policies, risks, controls, audits, and other processes to ensure adherence to the authoritative content.

Each authority document is defined in a record and the related lists on that record contain the individual conditions of the authority document.

The relationships of these authority document related list items are visible in the GRC Workbench in the Policy and Compliance Management application.

**Note:** You can add content reference tags to authority documents. Content reference tags allow you to filter records in order to more easily identify the content packs, integrations, and use case accelerators associated with the authority documents.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Citations

Citations contain the provisions of the authority document, which can be interrelated. Citations break down an authority document into manageable themes.

You can create citations or import them from UCF authority documents and then create any necessary relationships between the citations.

**Note:** You can add content reference tags to citations. Content reference tags allow you to filter records in order to more easily identify the content packs, integrations, and use case accelerators associated with the citations.

### Create a control indicator

Indicator data for controls, risk, and audit evidence are measured differently depending on the GRC application.

#### Before you begin

Role required: sn_compliance_admin, sn_compliance_manager

#### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Indicators** > **Indicators**.
   - **Risk** > **Indicators** > **Indicators**.
   - **Audit** > **Indicators** > **Indicators**.
2. Select **New**.
3. On the form, fill in the fields.

**Indicator form**

| Field | Description |
|---|---|
| Category | Select **Compliance Indicator** for a control indicator and **Risk Indicator** for a risk indicator. |
| Name | Name of the indicator. |
| Applies to | Entity related to the **Item**. |
| Owning group | Group that owns the indicator. |
| Owner | Indicator owner. |
| Number | Unique identification number. |
| Active | Option that indicates whether the indicator is active. |
| Item | Related control or risk. |
| Template | Related indicator template. |
| Override Template | Option that indicates whether to override the indicator template associated to this indicator |
| Last result passed | Option that indicates whether the last result passed. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| Next run time | Next collection time for indicator results. |
| Method | |
| Type | Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script.<br>◦ Manual<br>◦ Basic |
| Short Description | If Type is **Manual**, this field is present. Brief description of the issue. |
| Instructions | If Type is **Manual**, this field is present. Instructions for the collection of indicator results. |
| Value Mandatory | If Type is **Manual**, this field is present. |
| Passed/Failed | If Type is **Basic**, this field is present. Indicator passes or fails. |
| PA Threshold | If Type is **PA Indicator**, this field is present. The associated PA Threshold. |
| Script | If Type is **Script**, this field is present. Script that obtains the desired system information. |
| Supporting Data | |
| **Note:** Starting with Version 10.1, the actual historical data for the supporting data records from the indicator results or indicator tasks is displayed. Earlier, only the real-time state of the records collected could be viewed. | |
| Table | Use supporting data to gather supporting evidence from other applications. |
| Supporting data fields | Supporting data fields based on the selected table. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select **Submit**.

> **Note:** As a compliance manager or compliance admin, you can assign the indicator task to a user with Business User Lite role. If you assign a user with a Business User Lite role as an owner in the **Owner** field and **Execute** the indicator, an indicator task is created in the Open Tasks related list. This indicator task is assigned to the owner with the Business User Lite role.
>
> As a user with the Business User Lite role, you can navigate to **Policy and Compliance** > **Indicators** > **My Indicator Tasks** to view the indicator tasks that are assigned to you. You can view the indicator by selecting the information icon next to the Indicator field. You can also update the **Result** field, **State** field, **Value** field, **Additional comments**, and **Work notes** in the Indicator Task form.
>
> To accomplish similar tasks from the employee center, see GRC tasks in the employee center portal.

### What to do next

If you're implementing the Policy and Compliance Management software, then you've completed the required setup steps. Return to the Policy and Compliance Management setup checklist and proceed to the optional steps, as needed.

## Create a GRC indicator template

Compliance or risk managers create indicator templates from which many indicators can be created.

### Before you begin

Role required:

- sn_compliance.admin or sn_compliance.manager
- sn_risk.admin or sn_risk.manager
- sn_audit.admin or sn_audit.manager
- sn_grc.user

### Procedure

1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Indicators** > **Indicator Templates**.
   - **All** > **Risk** > **Indicators** > **Indicator Templates**.
2. Click **New**.
3. On the form, fill in the fields.

#### Indicator template form

| Field | Description |
|---|---|
| Name | Name of the indicator. |
| Description | Description of the indicator. |
| Category | Category for which you are creating an indicator template. For example, select **Risk Indicator Template** to create a risk indicator template. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Active | Option that determines whether the indicator template is active. |
| Method | |
| Type | Method used to determine the type of indicator template. The choices are as follows:<br>◦ **Manual**: Manual indicators are used for data that cannot be retrieved from a ServiceNow instance because it comes from an external system, such as customer data from a third-party sales system.<br>◦ **Basic**: Basic indicators are automated indicators based on an indicator source. The indicator source specifies a table and a frequency at which the scores from this table are saved.<br>◦ **Script**: Scripted indicators use a custom script to collect the data. |
| Result if the value meets or exceeds the target value | Result configuration field. The choices are as follows:<br>◦ **Passed**<br>◦ **Failed**<br>For example, assume you enter `100` in this field. If the indicator result output is more than 100, then the indicator status will pass or fail based on the value configured in this field. |
| Target Type | Type of the target value. The choices are as follows:<br>◦ **None**: Use this option if you do not want to set up any target or threshold for the indicator.<br>◦ **Percentage**: Use this option to determine the indicator result by a percentage value.<br>◦ **Count**: Use this option to determine the indicator result by a count value or total number. |
| Target | Value to determine if the indicator will pass or fail. |
| Instructions | Additional instructions for the template. |
| Value mandatory | Option to decide if a value must be compulsory in the indicator task for a manual indicator. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** This option appears only if **Manual** is selected from the **Type** field. This option is automatically selected if **Count** or the **Percentage** is selected from the **Target type** field. |
| Supporting Data | |
| **Note:** Starting with version 10.1, the actual historical data for the supporting data records from the indicator results or indicator tasks is displayed. Earlier, only the real-time state of the records collected could be viewed. | |
| Collect supporting data | Option to enable collecting supporting data or evidence every time the indicator runs. |
| Table | Table used for collecting supporting data. |
| Supporting data fields | Fields of the source table to be used for collecting the supporting data. |
| Sample collection type | Type of supporting data collection, such as count or percentage. |
| Sample size | Minimum number of records that must be used for collecting supporting data.<br><br>For example, a basic indicator could query a large table, returning thousands of records with each indicator execution. You do not need to save all of them; just a sample of those records. If you enter a sample size of 100, only 100 records are saved, even though the query returned thousands. |
| Basic Criteria | |
| Criteria | Criteria to filter the data from the source table. |
| Use reference field | Option to enable the use of the **Reference field**. |
| Reference field | Connection between the supporting data table and the **Applies to record** field of the entity. |
| Additional Criteria | |
| To create indicators with targets, use the advanced filter criteria. This section appears only when you select **Basic** from the **Type** field. This section is used to provide more filter criteria. | |
| Additional criteria | More criteria to filter the data to calculate the target value. This section only appears |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | when **Percentage** is selected from the **Target type** field. |
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| First run date | First collection time for indicator results. This field is automatically set based on when an indicator or an indicator template runs for the first time. The value in this field cannot be modified. |
| Next run date | Next run time to collect indicator results of all downstream indicators for this indicator template. |
| Due date duration (days) | Due date duration in days between the creation and due date of the indicator task and generation of its results.<br><br>The due date duration added to the creation date reflects as the **Due date** of the indicator task.<br><br>This field appears only when **Manual** is selected from the **Type** field.<br><br>For more information, see Performance enhancements for Indicator nightly job. |

4. When you have completed these entries, you can also view information on the following related lists:
   - Control Objectives/Risk Statements
   - Content References

   **Note:** The **Control Objectives/Risk Statements** tab enables you to reuse the same template for multiple control objectives or risk statements, or both of them.

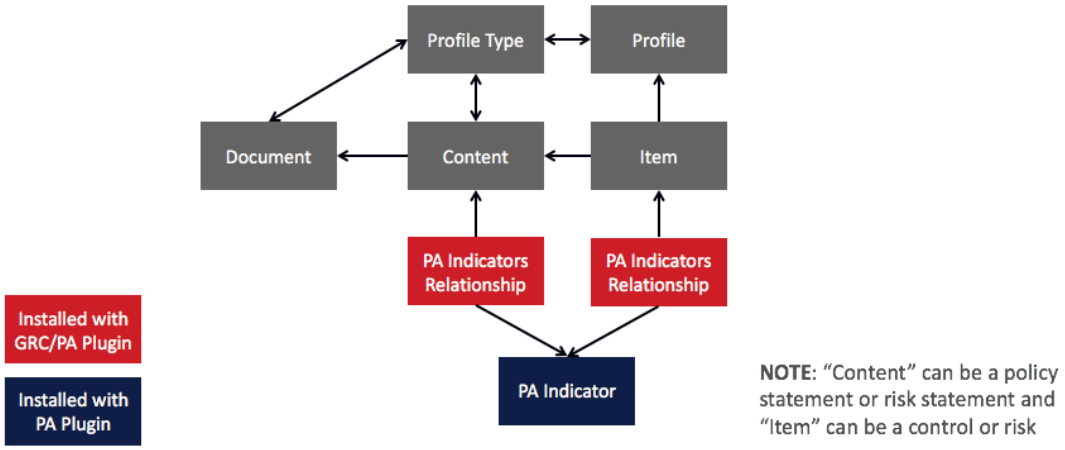
5. Select **Submit**.

## Monitor controls using GRC Performance Analytics Indicators

You can link Policy and Compliance Management content and items to Performance Analytics indicators, breakdowns, and thresholds. You can associate Performance Analytics indicators with control objectives and controls to view scorecards and trends and analyze current conditions and trends.

The risks and controls associated with a PA indicator or PA indicator/breakdown/element automatically monitor any PA threshold with the same PA indicator or PA indicator, breakdown, or element relationship. Any PA threshold breach is reported at the risk or control and Performance Analytics indicators relationship level within a breach counter.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## PA threshold breach impact

When a risk or control and Performance Analytics indicators relationship breach counter is different than zero (for example, a PA threshold with the same PA indicator or PA indicator, breakdown, or element relationship has breached), and if no opened issue exists, then an issue is created which is associated to the risk or control. Also for risks, the **Indicator failure factor** represents the number of risk and Performance Analytics indicators relationships with a breach counter different than zero.

## Reset all PA Indicator breach counters

Reset breach counters associated to a risk or control by clicking **Reset all PA Indicator breach counters** or opening the specific relationship and clicking **Reset Breach Counter**.

## GRC PA indicator breach reports

There are two reports for the reporting of breaches:

- Risk PA Indicator Breaches
- Control PA Indicator Breaches

### Activate GRC: Performance Analytics Integration

The GRC: Performance Analytics Integration plugin provides an integration between Performance Analytics and the Risk Management and Policy and Compliance Management applications. This plugin provides more insight into organizational risk and compliance performance.

#### Before you begin

Role required: admin

#### About this task

This plugin includes demo data and activates related plugins if they are not already active.

#### Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the plugin using the filter criteria and search bar.

   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Select **Install**, and then in the Activate Plugin dialog box, select **Activate**.

> **Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: `Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.`

### What to do next

After activating the GRC: Performance Analytics Integration plugin on an instance with customized related lists on content (risk or control objective) or items (risk or control), you may have to manually add the PA Indicator to content relationships and/or the PA indicator to item relationships.

Related topics

List of plugins

## Associate a PA indicator with a risk statement or control objective

You can associate Performance Analytics indicators with risk statements and policy statements to analyze trends related to the risk or policy.

### Before you begin

Role required: sn_risk.manager or sn_compliance.manager

### Procedure

1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Policies and Procedures** > **Control objectives**.
   - **All** > **Risk** > **Risk Library** > **Risk Statements**.
2. Open a risk statement or control objective.
3. In the **PA Indicators** related list, click **New**.
4. On the form, fill in the fields.

**PA Indicators form**

| Field | Description |
|---|---|
| PA Indicator | The performance analytics indicator to associate the Risk Statement or control objective with. |

5. Click **Submit**.
   On the risk statement or control objective form, in the **PA Indicators** related list, you see the associated indicator. You can optionally click **View Indicator** on the desired indicator to see the Performance Analytics scorecard of the indicator. The PA Indicator associations are carried over to all risks or controls associated to the original risk statement or control objective. Also, if the indicator has a breakdown that matches the risk or entity of the control (for example a Business Service breakdown), the **Breakdown** and **Element** fields for the relationship are automatically filled in.

## Associate a PA indicator with risks and controls

You can associate Performance Analytics indicators with risks and controls to analyze trends related to the entity that risk or control belongs to.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_risk.manager or sn_compliance.manager

### Procedure
1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Controls** > **All Controls**.
   - **Risk** > **Risk Register** > **All Risks**.
2. Open a risk or control.
3. In the **PA Indicators** related list, click **New**.
4. On the form, fill in the fields.

**PA Indicators form**

| Field | Description |
|---|---|
| PA Indicator | Performance analytics indicator to associate the Risk or Control with. |
| Breakdown | Break down to view a specific trend based on the breakdown element. |
| Element | Break down element to view a particular trend and scorecard.<br>**Note:** This field depends on the **Breakdown** field being populated. When visible, it is mandatory. |

5. Click **Submit**.
   On the Risk or Control form, in the **PA Indicators** related list, you see the associated indicator. You can optionally click **View Indicator** on the desired indicator to see the Performance Analytics scorecard of the indicator.

## Update associated GRC indicators for a set of items

You can update all the items belonging to a GRC content record so each item is individually related to the PA indicator.

### Before you begin
Role required: sn_risk.manager or sn_compliance.manager

### Procedure
1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Policies and Procedures** > **Control Objectives**.
   - **All** > **Risk** > **Risk Library** > **Risk Statements**.
2. Open a Risk Statement or Control Objective that has an associated Performance Analytics Indicator.
3. Click the **Update PA Relationships** related link.
   All the risks or controls related to the risk statement or policy statement are automatically associated with all the risk statement or policy indicators of the statement. Also, if the

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

indicator has a breakdown that matches the risk or entity of the control (for example a Business Service breakdown), the **Breakdown** and **Element** fields for the relationship are automatically filled in.

## Manage evidence requests

Evidence request is used by audit and compliance teams for requesting supporting documents during an audit. Auditors and compliance teams require these documents from the first line of defense.

Evidence request: Evidence is all the information used by an auditor in determining the audit opinion. Evidence includes the information contained in the accounting records underlying the financial statements and other information. Evidence is cumulative in nature. It includes evidence obtained from audit procedures performed during the audit. Evidence may also include audit evidence obtained from other sources such as, previous audits.

An evidence request is frequently introduced during the audit preparation or planning phase after the audit announcement. The documents requested are used by the audit team to understand the in-scope controls and processes, and to begin fieldwork testing. As an audit progresses through various stages, the audit team frequently adds new requests to the list. The compliance teams use the collected evidence for control testing.

Starting with version 11.0.2 release, an unplanned evidence request is supported by the Audit Management and Policy and Compliance Management applications in the following ways.

- Evidence can be requested from an engagement and all audit tables. To understand how to request evidence, see Request evidence for audit.
- Compliance teams can request evidence from control owners, business stakeholders, and process owners.
- Audit teams can request evidence from control owners, business stakeholders, process owners, and compliance teams.
- Assigned users can provide evidence directly from the Service Portal.
- Managers can approve evidence requests based on various criteria, such as confidentiality and criticality.
- Improved communication channels between requesters and assignees streamline the approval process.
- Improved confidentiality constraints prevent unauthorized persons from viewing request information.

### Evidence request workflow and users

Evidence request helps customers to electronically request the information that they need from the first and second line of defense. The individuals being audited can then immediately upload their documents to the system, significantly reducing manual processing time.

The evidence request workflow is as follows:

1. An audit user with the sn_audit.user role requests evidence and assigns the request to another user. This requester can either request the evidence for themselves or raise a request on behalf of another audit user or GRC user. If the requester determines that an evidence task has been created erroneously, then the requester can cancel that particular evidence task. The ability to cancel the evidence request is available when the request is in **Draft** state. A requester can cancel the evidence request tasks any time until the tasks reach the **Review** state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. After you create an evidence request, you must create evidence collection records and then the requester must request evidence. Evidence Collection records contain the evidence collection instructions, assigned to, and assignment group. On clicking **Request Evidence**, evidence request tasks are generated and they are assigned to a group or user.
3. The assignee then receives an email with the link to provide the requested evidence.

   **Note:** If the requester changes the assignee after requesting evidence, then the original assignee can no longer view the request. Only the person who is assigned the request can view the request. This feature ensures confidentiality.

4. The assignee can either attach the requested evidence or provide a URL or location that contains the required evidence.
5. The assignee can also add an approver for verifying and approving the evidence. Adding approvers is necessary if the evidence is sensitive and confidential in nature.
6. The approver can then review the evidence and either approve it, request revision, or request further details about the evidence.
7. If the approver approves the evidence, the requester receives the evidence and can process it further.
8. The requester can then review the evidence and do one of the following:
   - accept the evidence.
   - request for its review.
   - request further details about the evidence.
   - cancel the evidence request if it is not required anymore.
   - delete the request.
9. If the requester accepts all the evidence tasks, the request is closed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The evidence request workflow is shown in the following

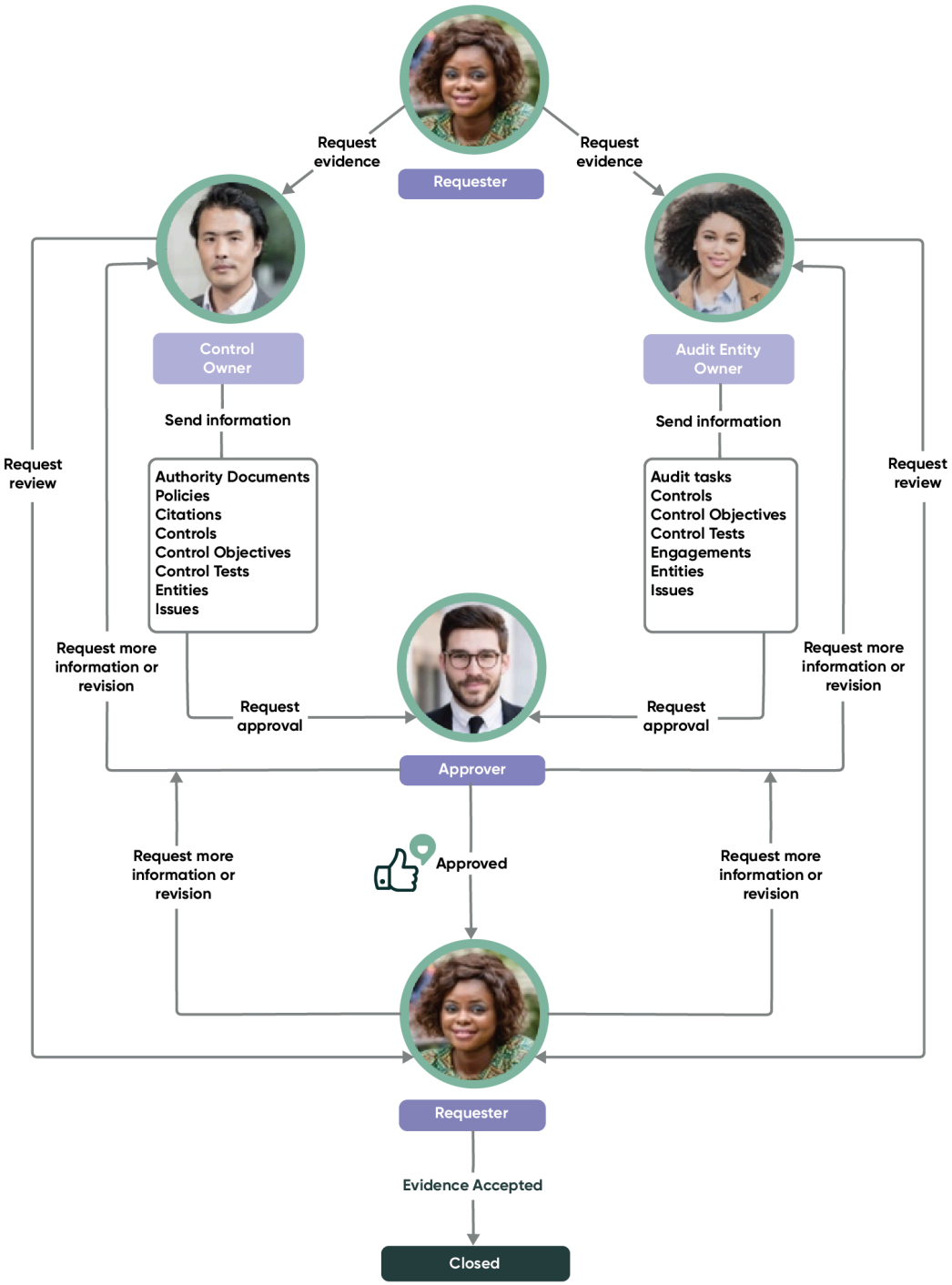



figure:

The following table describes the roles and their responsibilities during the evidence request workflow:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Evidence request users, responsibilities, and requirements

| User | Responsibilities | Requirements |
|---|---|---|
| Internal auditor | • Perform audit testing.<br>• Request audit testing.<br>• Review all audit findings and the evidence collected. | • Visibility into compliance and risk activity.<br>• A job queue (pending, current, upcoming) to plan their team efforts.<br>• Track and monitor audit findings.<br>• Track and monitor audit activities. |
| Compliance manager, Audit manager | • Can request evidence.<br>• Request compliance test evidence.<br>• Review all findings and evidence collected. | • Visibility into compliance activities.<br>• A job queue (pending, current, upcoming) to plan their team efforts.<br>• Track and monitor compliance findings. |
| Compliance user, Control owner | • Ensure that the controls are implemented.<br>• Attest to the controls.<br>• Test the controls.<br>• Provide audit evidence requested by the auditor. | • A job queue to direct their day-to-day activities.<br>• Track the time spent and performance of activities and tasks they own.<br>• Ensures the task they own and additional request from the auditor is fulfilled. |

### Request evidence during audits

Request evidence at any stage during an audit. The details about the items for which evidence is requested are also provided to the person responsible for providing the evidence.

## Before you begin

Role required: sn_audit.user

## About this task

An evidence can be requested in the following three ways:

My Evidence

By creating an evidence record from the **My Evidence** module.

Request Evidence

From the Entity, Control, Audit Task, Control Test Issue, and Other Issues related lists in an engagement record. To request evidence from these sources, navigate to **Audit** > **Engagements** > **My Engagements**. Open the engagement record, and select the related list from which you want to request evidence. From the

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Action on selected rows** list, select **Request Evidence**. Here, you can either create a new evidence request or add more requests to an existing evidence request. The Evidence request is created but not evidence request tasks. For more information on adding existing evidence, see Reuse existing evidence from the related items of an engagement.

Entity, Control, Control Objective, Control Test, Engagement, Issue tables

From tables such as Entity, Control, Control Objective, Control Test, Engagement, Issue. However, when the users request evidence from these tables, the evidence request is created not the actual evidence request task. The users must navigate to the evidence request record that is generated and then add evidence request tasks.

In this procedure, the method to request evidence from the **My Evidence** module is described.

## Procedure

1. Navigate to **Audit** > **My Evidence Request**.
2. Click **New**.
3. On the form, fill in the fields.

**Evidence Request form**

| Field | Description |
|---|---|
| Number | Unique number of the evidence request. |
| Requester | User requesting evidence. This field is automatically populated. |
| Requested on behalf of | User for whom evidence is being requested. |
| Assignment group | Group assigned to provide evidence. |
| Assigned to | User responsible for providing the evidence. |
| State | State of the request. The default state is **Draft**. |
| Type | Type of evidence that is created. Can be either Audit or Compliance. |
| Request reason | Reason for requesting evidence. |
| Watch list | Users interested in viewing the evidence collected. If a person is added on the watch list, they can navigate to **Audit** > **Evidence Request** > **Watched Evidence Requests** to view the requests. |
| Name | Name of the evidence request. |
| Description | Detailed description of the evidence request. |
| Schedule | |
| Due date | Expected date of evidence submission. |
| Opened | Date the request is opened. This date is automatically updated. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Closed | Date the request is closed. This date is automatically updated. |
| Activity | |
| Work notes | Type any notes that might be required. |
| Activities | Activity log for the request. |

4. Save the form.
   The Evidence Collection Details related list appears. This related list is used to list the items for which evidence is requested.
5. Click **New**.
6. On the form, fill in the fields.

**Evidence Collection Detail form**

| Field | Description |
|---|---|
| Evidence request | Unique number of the evidence request task. |
| Evidence for | Record for which evidence is requested.<br><br>Lists all tables to which the evidence is applied. |
| Name | Evidence collection detail name. |
| Assignment group | Group assigned to provide evidence. The users of this group must have the sn_grc.business_user roles. |
| Assigned to | User responsible for providing evidence. |
| Evidence collection instructions | Instructions for providing evidence. For example, list of supporting documents, files, and so on. |

7. Click **OK**.
8. Click **Submit**.
9. Click **Request Evidence**.
   When an evidence request is already in the Work in Progress state, and a new evidence collection detail is added, then evidence request task is sent to the assignee immediately. The Evidence related list appears with the list of evidences and the person who is assigned the request receives an email notification to provide the requested evidence. Also, the state of the request changes to **Work in Progress**.
10. Navigate to **Audit** > **Evidence Request** > **My Evidence Request Tasks**.
11. Open the record for which you want to provide evidence.
12. Click **Accept Work**.
13. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Evidence form

| Field | Description |
|---|---|
| Number | Number of the evidence request. This value is generated by default. |
| Requester | User requesting evidence. This value is generated by default.<br><br>If you are the approver, requester, watch list member, or user in the Assigned to field, then you can edit the details in the **Watch list**, **Name**, and **Description** fields when the evidence is in **New** or **Work in progress** states. |
| Requested on behalf of | User for whom evidence is being requested. This value is generated by default. |
| Assignment group | Group assigned to provide evidence. The users of this group must have the sn_grc.business_user roles. |
| Assigned to | User responsible for providing the evidence. This value is generated by default. |
| State | State of the request. |
| Substate | None. This value is generated by default. |
| Request reason | Reason for requesting evidence. |
| Approvers | Users to approve evidence before it is returned to the requester for review. Usually, an approver is the manager of the person providing the evidence. |
| Watch list | Users interested in viewing the evidence collected. |
| Name | Name of the evidence request. The name defaults to Evidence collection details name. |
| Description | Detailed description of the evidence request. The description defaults to the description given in the Evidence request form. |
| Request Details | |
| Evidence request | Unique ID of the evidence request associated with the task. This value is generated by default and is fetched from the record that was created to request evidence. |
| Evidence for | Record for which the evidence is requested. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Evidence for description | Description of the record for which the evidence is being requested. This value is generated by default and is fetched from the record that was created to request evidence. |
| Evidence collection instructions | Instructions to collect the evidence.<br><br>If you are the manager or requester, you can edit this field when the evidence request task is in work in progress state. |

14. To request approval for the attached evidence, click **Request Approval**.
15. If no approvers are required, click **Request Review**.
16. Navigate to **Audit** > **Evidence Request** > **My Approvals**.
17. Open the record for which you want to approve evidence.
18. Review the attached evidence on the form and click one of the following options:

| Option | Description |
|---|---|
| **Approve** | Approve the attached evidence. The requester gets the evidence provided. |
| **Request Revision** | Request that the attached evidence be reviewed. Enter comments when you request revision. The assignee gets a notification to review the attached evidence. |
| **Request Information** | Seek more information and details about the attached evidence. The assignee gets a notification to provide more information about the attached evidence. |

19. Navigate to **Audit** > **Evidence Request** > **My Pending Reviews**.
20. On the Evidence form, review the attached evidence, and click one of the following options:

| Option | Description |
|---|---|
| **Accept Evidence** | Accept the evidence that is provided. |
| **Request Revision** | Request for the evidence to be reviewed, if it is not appropriate, or modified. |
| **Cancel** | Cancel the evidence request task. |
| **Delete** | Delete the evidence request task. |

21. Navigate to the form for which you want to display the **Evidence Request** related list.
22. Right-click in the form header, and click **Configure** > **Related Lists**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

23. Locate the **Related Evidence** item in the **Available** box and move it to the **Selected** box.
24. Click **Save**.

### Reuse existing evidence from the related items of an engagement

Inform the audit and compliance user about the evidences that are already existing for the related items of an engagement. You can add such an evidence, if it is already existing for any of the related item table of an engagement for which you are requesting an evidence.

#### Before you begin

Role required: sn_audit.user

#### About this task

For an engagement, an evidence can be created on Entity, Control, Audit Task, Control Test Issue, Other Issues, or any of the related item table. If there are existing evidences, then the Request Evidence pop-up displays a message that there are existing evidences that you might want to add.

**Note:** Evidences that are directly created on a related item, and existing evidences that are in **Closed** state as well as those that are within six months from the due date of evidence response can only be added.

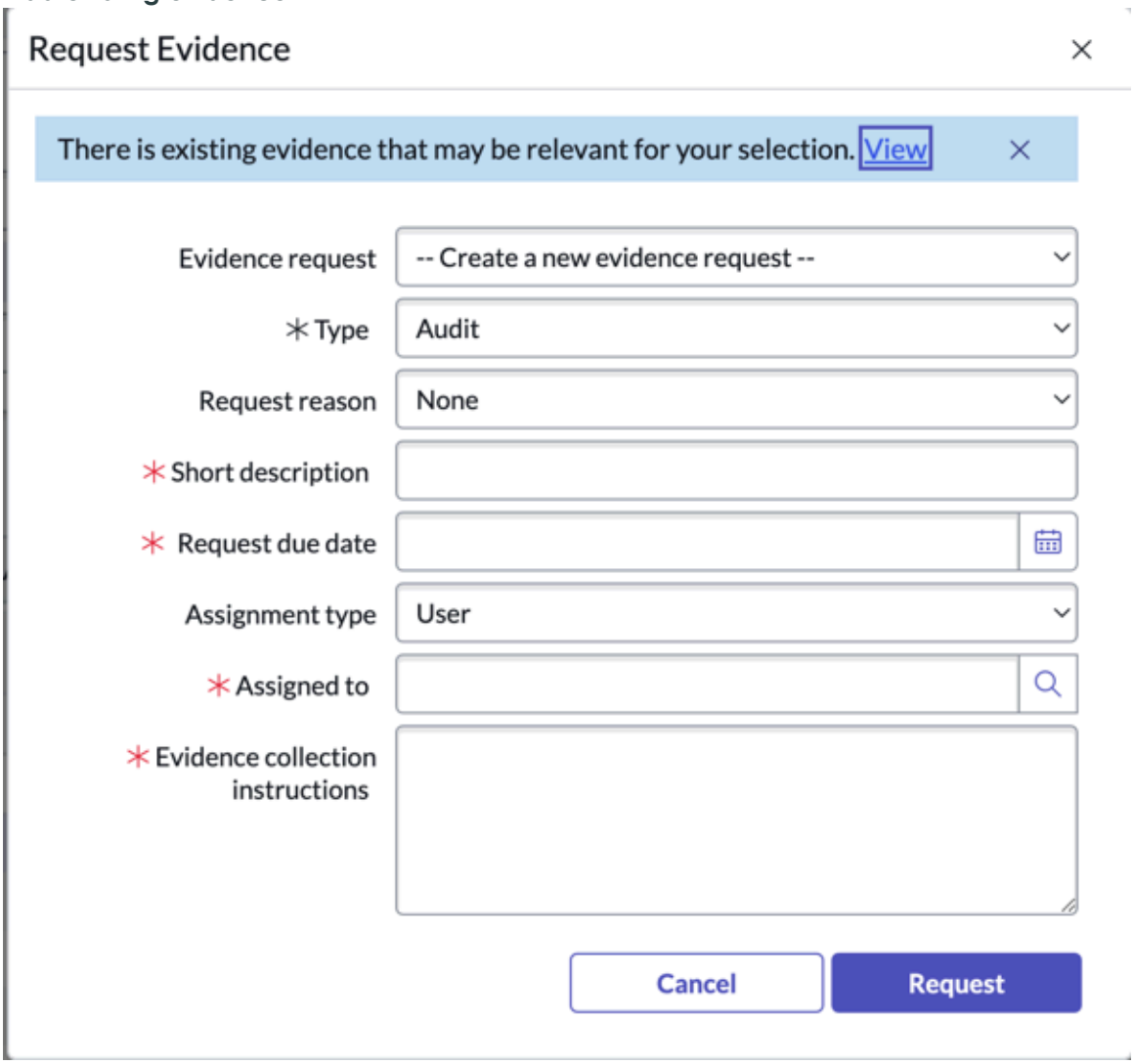
The logged in user must also have access to the engagement for which evidence records exist or must be the user who has access to the engagement record to view and add them. If the logged in user does not have access to those records, although there are evidences existing on those related items, they are not displayed for the user to add.

#### Procedure

1. Navigate to **All** > **Audit** > **Engagements** > **All Engagements**.
2. Click to open an engagement.
3. Select the related list from which you want to request evidence.
4. From the **Action on selected rows** list, select **Request Evidence**.
   You can either create a new evidence request or add existing evidence request. The Evidence request is created but not evidence request tasks.
5. To create a new evidence request, enter details on the Request Evidence pop-up and click the **Request** button.
6. To view existing requests, click **View** in the message.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Add existing evidence**




**Note:** If there is no existing evidence, then the message does not appear in the Request Evidence pop-up.

7. To view all existing evidences created on the related items, click the Evidence related list. When the evidence is in **Closed Complete** state, the UI action buttons such as **New**, **Add existing evidence**, **Remove**, and **Delete** are disabled. You can perform these UI actions only when the engagement or any other audit and compliance object is in an active state.
8. To associate the evidence, click the **Add Existing Evidence** button and select the evidence.

   **Note:** The **Add Existing Evidence** button is only available in the Evidence related item of an Engagement form and not in any other compliance or audit objects of the Classic environment.

9. To remove the association of the evidences linked to the engagement, select the evidences in the Evidence related list and click **Remove** in the **Actions on selected rows** list.

   **Note:** The remove action only removes the association of the existing evidences from the engagement and does not remove the evidence record from the database.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Provide requested evidence

Provide evidence when you are requested. When evidence is requested, the person who must provide the evidence receives an email. The process to provide the evidence begins.

## Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

## About this task

When the assignee receives the email to provide the requested evidence, the assignee can either provide the requested evidence or reassign the request to another user. The assignee can also add approvers before sending the requested evidence to ensure additional security of the evidence. If the assignee reassigns the request to some other user, the original assignee can no longer view the request. If the evidence provided does not need an approver, then the assignee can directly request a review of the evidence, and the requester gets a notification to review the evidence.

## Procedure

1. Navigate to **Audit** > **Evidence Request** > **My Evidence Request Tasks**.
2. Open the record for which you want to provide evidence.
3. Click **Accept Work**.
4. On the form, fill in the fields.

### Evidence form

| Field | Description |
|---|---|
| Number | Number of the evidence request. This value is generated by default. |
| Requester | User requesting evidence. This value is generated by default.<br><br>If you are the approver, requester, watch list member, or user in the Assigned to field, then you can edit the details in the **Watch list**, **Name**, and **Description** fields when the evidence is in **New** or **Work in progress** states. |
| Requested on behalf of | User for whom evidence is being requested. This value is generated by default. |
| Assignment group | Group assigned to provide evidence. The users of this group must have the sn_grc.business_user roles. |
| Assigned to | User responsible for providing the evidence. This value is generated by default. |
| State | State of the request. |
| Substate | None. This value is generated by default. |
| Request reason | Reason for requesting evidence. |
| Approvers | Users to approve evidence before it is returned to the requester for review. Usually, |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | an approver is the manager of the person providing the evidence. |
| Watch list | Users interested in viewing the evidence collected. |
| Name | Name of the evidence request. The name defaults to Evidence collection details name. |
| Description | Detailed description of the evidence request. The description defaults to the description given in the Evidence request form. |
| Request Details | |
| Evidence request | Unique ID of the evidence request associated with the task. This value is generated by default and is fetched from the record that was created to request evidence. |
| Evidence for | Record for which the evidence is requested. |
| Evidence for description | Description of the record for which the evidence is being requested. This value is generated by default and is fetched from the record that was created to request evidence. |
| Evidence collection instructions | Instructions to collect the evidence.<br><br>If you are the manager or requester, you can edit this field when the evidence request task is in work in progress state. |

5. To request approval for the attached evidence, click **Request Approval**.
6. If no approvers are required, click **Request Review**.

### Approve evidence before evidence review

Approve the evidence being provided before the requester views the evidence. When evidence is provided in response to an evidence request, the evidence may need an approval before the evidence is sent back to the requester. This ability ensures security and confidentiality of the evidence.

#### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

#### About this task

After receiving a request to approve evidence, an approver can do one of the following:

- Approve the request if there are no issues or concerns.
- Request revision of the evidence attached in case it is not correct or needs rectification.
- Request information if the approver wants more details about the attached evidence.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **Audit** > **Evidence Request** > **My Approvals**.
2. Open the record for which you want to approve evidence.
3. Review the attached evidence on the form and click one of the following options:

| Option | Description |
|---|---|
| **Approve** | Approve the attached evidence. The requester gets the evidence provided. |
| **Request Revision** | Request that the attached evidence be reviewed. Enter comments when you request revision. The assignee gets a notification to review the attached evidence. |
| **Request Information** | Seek more information and details about the attached evidence. The assignee gets a notification to provide more information about the attached evidence. |

## Accept, reject, or cancel evidence request

Accept, reject, or cancel an evidence request when you receive the evidence you requested. After requesting an evidence request, when the requester receives the evidence, the requester can accept, reject, or cancel the evidence request.

### Before you begin

Role required: sn_compliance.user

### Procedure

1. Navigate to **Audit** > **Evidence Request** > **My Pending Reviews**.
2. On the Evidence form, review the attached evidence, and click one of the following options:

| Option | Description |
|---|---|
| **Accept Evidence** | Accept the evidence that is provided. |
| **Request Revision** | Request for the evidence to be reviewed, if it is not appropriate, or modified. |
| **Cancel** | Cancel the evidence request task. |
| **Delete** | Delete the evidence request task. |

## Review related evidence

The Evidence Request feature includes a related list called Related Evidence, which it not visible by default. This related list provides a list of evidence that is not directly requested for the current record, but is associated to a related record. For example, the Related Evidence list on the Control Objective form shows evidence requested for associated controls.

### Before you begin

Role required: admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

The Related Evidence related list is available to a wide variety of forms throughout the Evidence Request feature; however, it is not visible in the base system. You can personalize any of the forms in which is it available, but keep in mind that activating this related list can impact system performance.

**Tables that can display the Related Evidence related list**

| Table name | Type of related evidence displayed |
|---|---|
| Authority document | Evidence request tasks created on the citations mapped to this authority document. |
| Citation | Evidence request tasks created on the control objective associated to the citation. |
| Control | Evidence request tasks created on the control test mapped to the control and Issues created for the control. |
| Control objective | Evidence request tasks created on the controls associated to the control objective. |
| Control test | Evidence request tasks created on the controls associated to the control test. |
| Engagement | Evidence request tasks created on the entities, controls, control tests, audit tasks, control test issues, and issues mapped to the engagement are displayed. |
| Entity | Evidence request tasks created on the controls associated to the entity, Issues created on the entity. |
| Policy | Evidence request tasks created on the control objective associated to the policy. |

### Procedure

1. Navigate to the form for which you want to display the **Evidence Request** related list.
2. Right-click in the form header, and click **Configure** > **Related Lists**.
3. Locate the **Related Evidence** item in the **Available** box and move it to the **Selected** box.
4. Click **Save**.

## Performing compliance tasks in Compliance Workspace

Starting with Version 13.0.0, a new workspace has been introduced for the GRC: Policy and Compliance Management application. The new workspace provides you with an improved User Experience (UX) and a simplified user journey.

**Note:** Compliance Workspace has a dependency on GRC: Policy and Compliance Management application and the latter is automatically installed when the workspace plugin is installed.

To know more about Compliance Workspace, see Exploring GRC Compliance Workspace. For persona-based Compliance Workspace pages, see:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Compliance Home page for the compliance manager
- Compliance Home page for the compliance analyst
- Compliance Home page for the IT compliance manager

## Exploring GRC Compliance Workspace

Compliance Workspace is a unified interface where you can manage all your tasks related to policies, control objectives, controls, issues, and policy exceptions.

## Compliance Workspace overview

The highlights of the Compliance Workspace are:

Reimagined user experience

From the minute you navigate to the Compliance Workspace home page, all the tasks that you can possibly do in the workspace are streamlined to fulfill your business goals.

Workspace designed for different compliance user roles

Distinct page views for the exclusive activities of a Corporate compliance manager and Corporate compliance analyst.

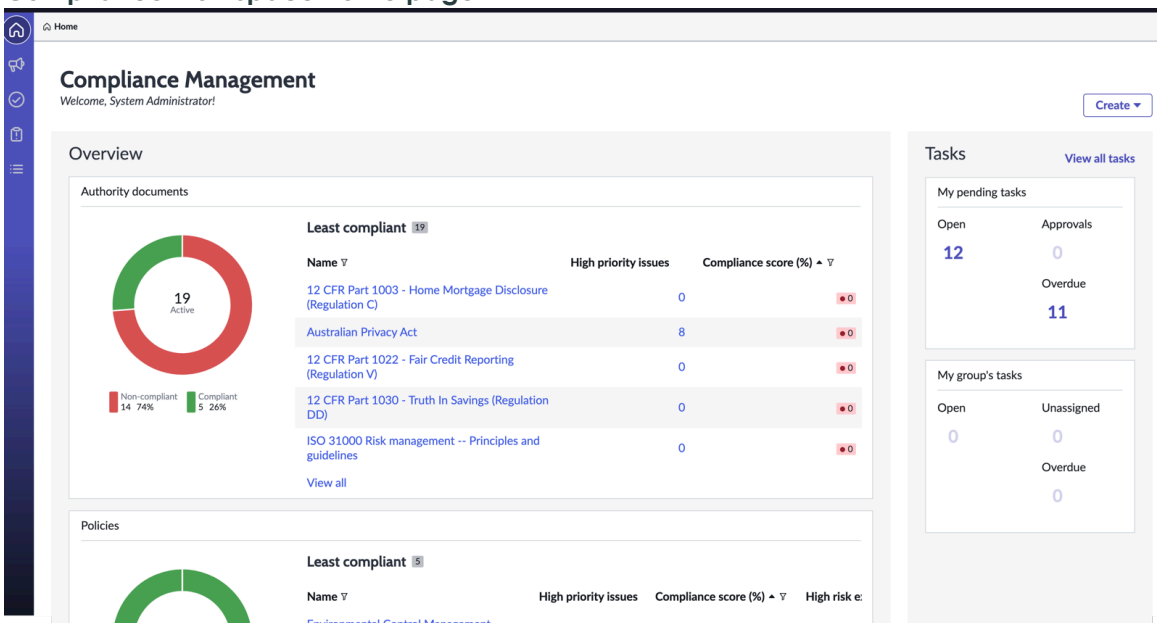
Home page with different sections

Overview

Donut charts display the categorical data of compliant and non-compliant authority documents, policies, and entities.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Compliance workspace home page




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Control assurance

Displays the donut charts, grouping indicators by status, and attestations by state. Control test horizontal bar grouped by control and classification stacked by control effectiveness.

Tracking

Displays controls widget grouped by state and stacked by classification. Issues horizontal bar grouped by state and stacked by priority.

**Note:** Control tests widget is visible only when the audit plugin is activated.

The base condition to filter issues is that the Classification must be Compliance or empty, or in the case where the issue has an m2m association with an engagement, the logged-in user must be one of the three users, such as an auditor, engagement lead, or approver. The base filter conditions are applicable for the Compliance Workspace and define the compliance issues.

Tasks

View your pending tasks and the group's tasks. You can navigate to the unified tasks page by clicking the **View all tasks** link.

Unified Tasks page

Track your tasks and team's tasks from a single interface. View your tasks by categories, filter them by various parameters, monitor those tasks that you've initiated, and track through the watchlist.

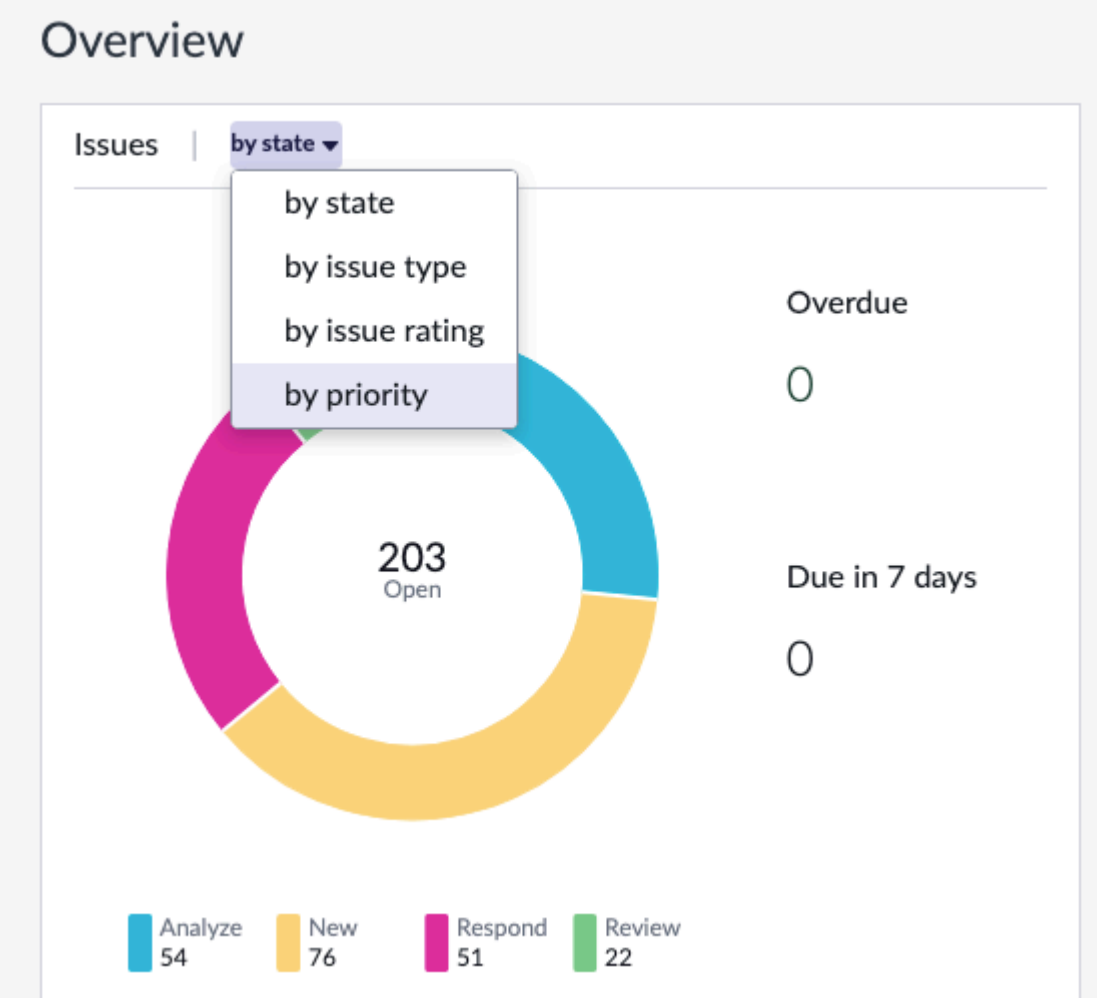
Issues overview

A dedicated page to view and know all about the issues.

Issues overview page provides an overview of issues that are open, overdue, and due in the next seven days. You can group issues based on its state, issue type, issue rating, or priority. Use the tracking section to get the status of the remediation tasks and exceptions. Get the trend of issues that are open and closed over time in the Performance section.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Issues overview**




Lists

List view of all compliance-related records, providing the summary of the record in a single view that helps in your analyses and take an informed decision.

**Note:** The **Control tests** widget, **Regulatory changes** widget, and **Domain compliance status** section appear with the installation of audit, regulatory change management, and privacy management plugins, respectively. For more information, see Other GRC plugins for an overall view.

## Roles in the Compliance Workspace

The targeted users of the Compliance Workspace are the corporate compliance managers and the corporate compliance analysts. For more information on the roles, the responsibilities, and the tasks that the users can accomplish in the Compliance Workspace, see

- Compliance Home page for the compliance manager.
- Compliance Home page for the compliance analyst.
- Compliance Home page for the IT compliance manager.

### Compliance Home page for the compliance manager

The compliance manager home page in the Compliance Workspace gives a complete overview of the compliance posture of the organization. The workspace helps the

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

compliance manager to centrally manage internal standards, policies, and control processes that match the external regulatory standards.

Compliance manager most often reports to a compliance director and ensures that the company complies with organizational and industrial regulations and standards.

The user persona may vary across organizations, however, a corporate compliance manager, IT compliance manager, compliance manager, or compliance analyst, depending on the organizational structure, can be tasked with ensuring that the organization is complying with policies and regulations.

## Responsibilities of a compliance manager

The compliance manager must

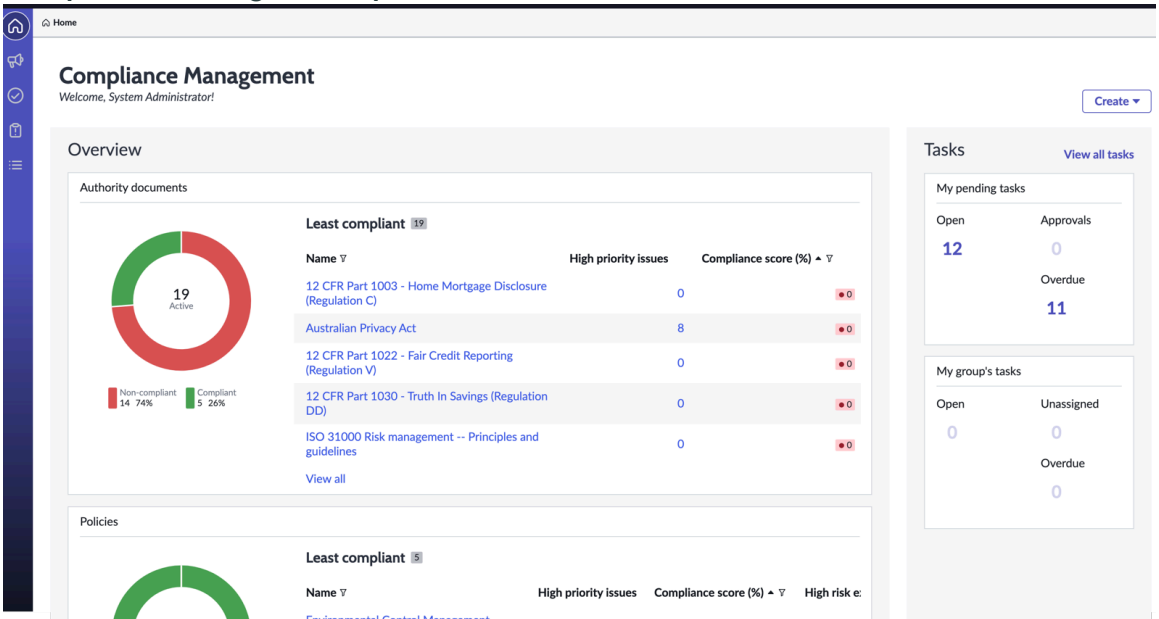
- Ensure that all policies and regulations are being followed.
- Create and maintain policies up to the level of defining and applying controls.
- Approve and track policy exceptions and issues.
- Manage the team appropriately.

## Compliance Workspace for compliance manager tasks

To fulfil the above responsibilities, a compliance manager has certain daily and weekly functional tasks that can be performed in the compliance workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Compliance manager workspace




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Use the Overview section to review the authority documents, policies, and entities and know their compliant status. Get the list of least compliant authority documents, policies, and entities, priority of the issues created, and their compliance score.
- Review compliance tasks such as controls, control attestations, indicator tasks, ongoing and overdue control test count in the control assurance section.
- Monitor and analyze new key controls and track the performance of existing controls.
- Identify past due tasks, recurring issues, inadequate remediation strategies.
- Get an overview of all your compliance tasks – pending tasks and group's tasks.
- Track the changes done to the authority documents, regulations, and policies.

As a compliance manager, you can create authority documents, citations, policies, control objectives, controls, indicator tasks, acknowledgement campaigns, issues, policy exceptions, and engagements.

To help the compliance manager attend to tasks that need immediate action, the compliance records in the overview section are listed in an order starting from the least compliant ones. The data displayed for control tests, indicators, and attestations in the control assurance section help the compliance manager to prioritize the tasks as well. Tracking of issues, acknowledgement campaigns, and policy exceptions can be managed effectively.

## Other GRC plugins for an overall view

As the compliance manager requires an overall view of all compliance tasks, they can view the privacy management and regulatory change management application domains as well in the compliance manager home page. However, you require the following plugins to be installed for certain widgets to be displayed on the home page.

- GRC: Audit Management for the control tests widget in the Control assurance section.
- GRC: Regulatory Change Management for the Regulatory changes widget in the Tracking section. The logged in user must also have the RCM manager role (sn_grc_reg_change.manager).
- GRC: Privacy Management for the Domain compliance status section. The logged in user must also have a privacy manager role (sn_privacy.manager).

### Compliance Home page for the compliance analyst

The compliance analyst home page in the Compliance Workspace enables the compliance analyst to track compliance activities and helps compliance managers to ensure that the organization is compliant with various regulations and policies.

## Responsibilities of a compliance analyst

The compliance analysts oversee specific areas of compliance including specific policies, regulations, and related compliance activities. Therefore, the filter option help them to filter the compliance records based on the required criteria. They can view and work on the tasks that they are assigned to.

- Analyze and update the existing policies and related documents.
- Implement policies and controls when assigned.
- Monitor the performance of controls.
- Schedule and follow up attestations.

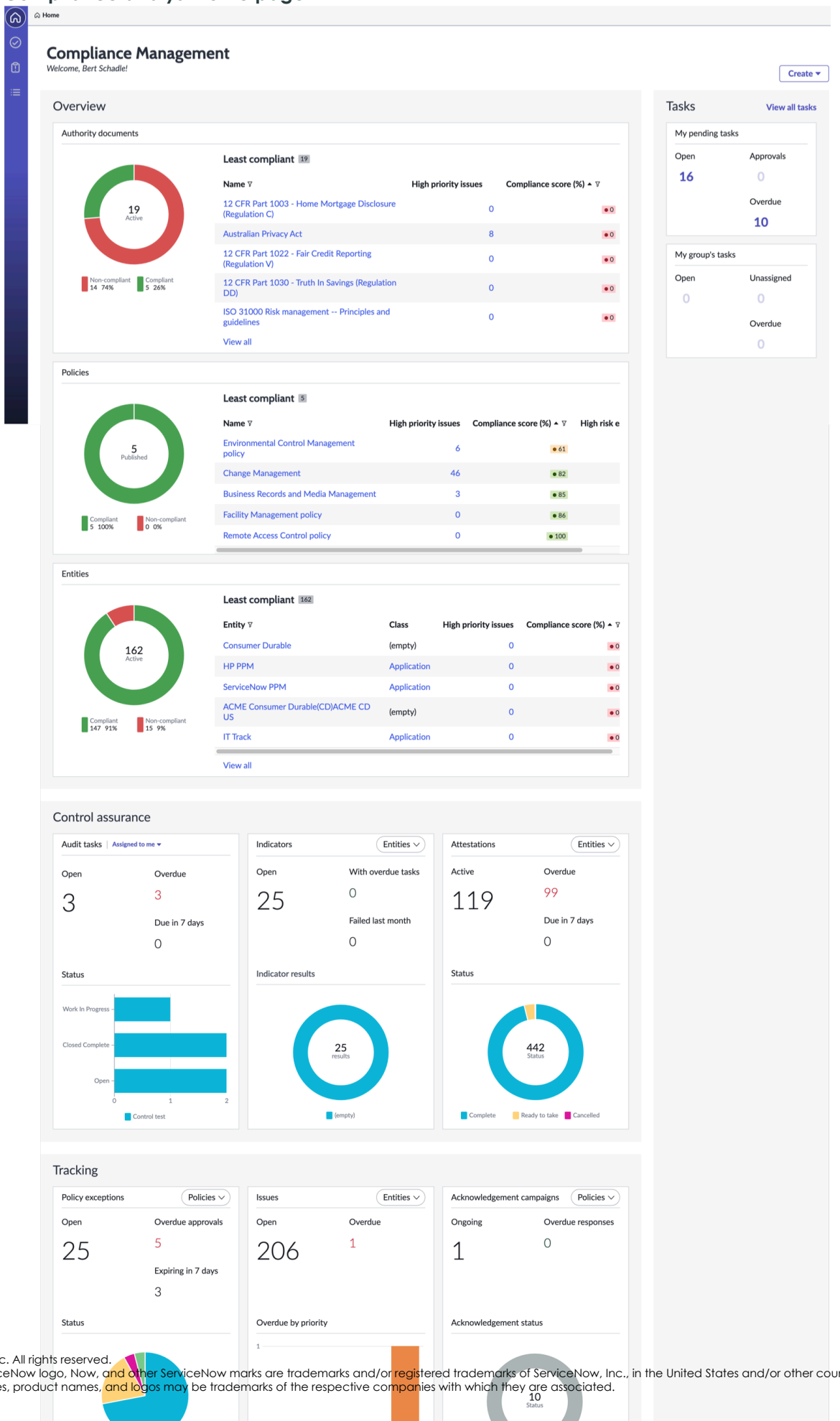
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Compliance Workspace for compliance analyst tasks

The compliance analyst home page is designed to fulfil the above tasks of an analyst. Although the Home page is similar to the compliance manager home page, yet there are features that are unique to help the analysts perform their tasks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Compliance analyst home page




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The compliance analyst Home page provides a personalized experience for a corporate compliance analyst to manage their work.

Overview

Provides a summary of the overall compliance stance of the organization.

Authority documents

The widget displays the overall count of authority documents, summing up the counts of compliant and non-compliant authority documents. The section also gives you details of high priority issues and the compliance score percentage. Clicking the name of the authority document takes you to a detailed overview of the document showing its compliance status and tracking details.

Policies

In addition to the count of compliant and non-compliant policies and the list of least compliant policies with high priority issues and compliance score, this section also provides the number of high risk exceptions for each listed policy.

Entities

Provides the total count of active entities, and a list of least compliant entities along with their entity class. Click the name of an entity to know its compliance status and tracking details.

Control Assurance

Provides an overview of testing and monitoring controls. By default, the audit tasks are filtered and displayed based on the **Assigned to me** condition of the logged in user. Whereas, the analyst can filter the indicators and attestations based on the entities that they manage.

Tracking

Provides a summary of important and open issues, tasks, and exceptions and helps the analyst to manage policy exceptions and issues. Since the analyst is required to understand the policy exceptions and issues created on the policies that is assigned to them, they can apply the filter on the required policies and view the exceptions and issues created on these policies. Similarly, the analyst can select specific policies to view its campaign details.

Tasks

Provides a summary of My pending tasks and My group's tasks – the job queue directs their day-to-day activities.

Quick links

Enables the analyst to create new records such as control objectives, controls, acknowledgement campaigns, issues, and policy exceptions.

### Compliance Home page for the IT compliance manager

The Compliance Workspace provides an exclusive home page for the IT compliance manager to view the IT-related risk and compliance data. The workspace helps the IT compliance manager to centrally manage internal standards, policies, and control processes that are exclusively IT-related to comply with the external regulatory standards.

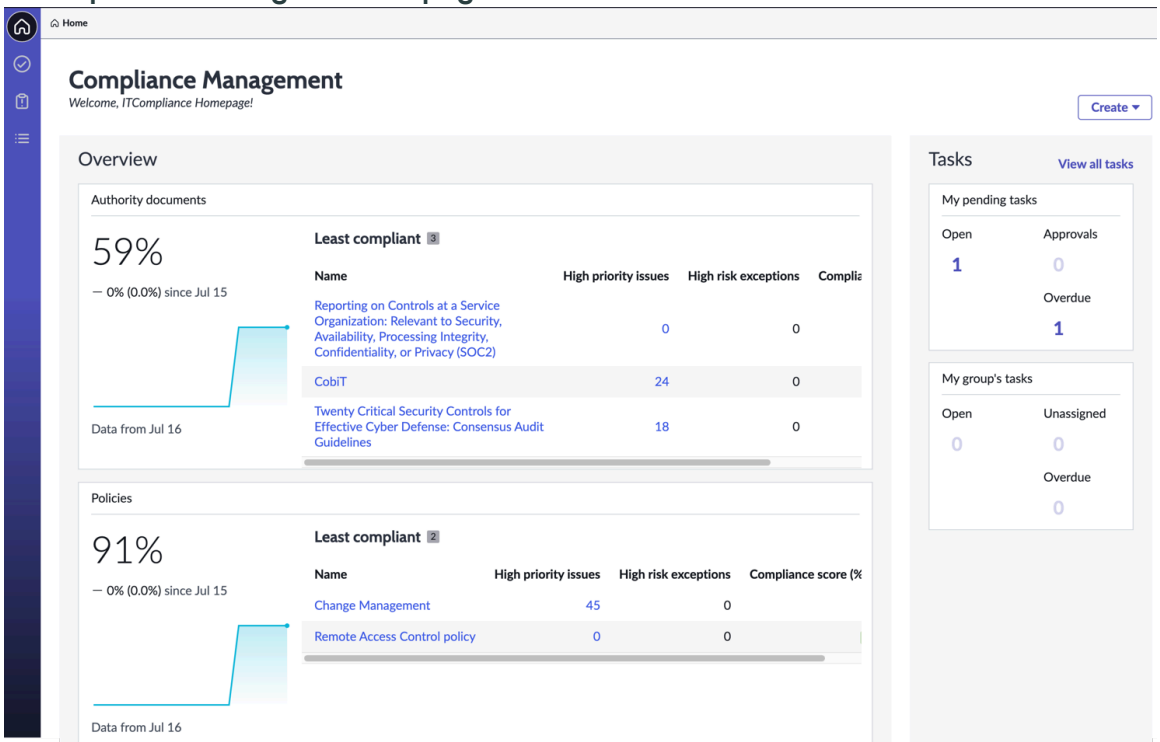
## Configuring IT Compliance Workspace

- To set up the IT Compliance Home page, see Configuring IT compliance workspace.
- For information on the tables that support IT compliance workspace and the user roles, see Components installed with Policy and Compliance Management.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# IT Compliance Home page

## IT compliance manager's home page




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Overview

The compliant percentage of IT-related authority documents, IT-related policies, and IT-related entities are indicated by PA indicator widgets.

Control effectiveness

This section provides reports, gathering real-time information, on IT-related controls, the indicators that run on the IT-related controls, and the attestations that are associated to those controls.

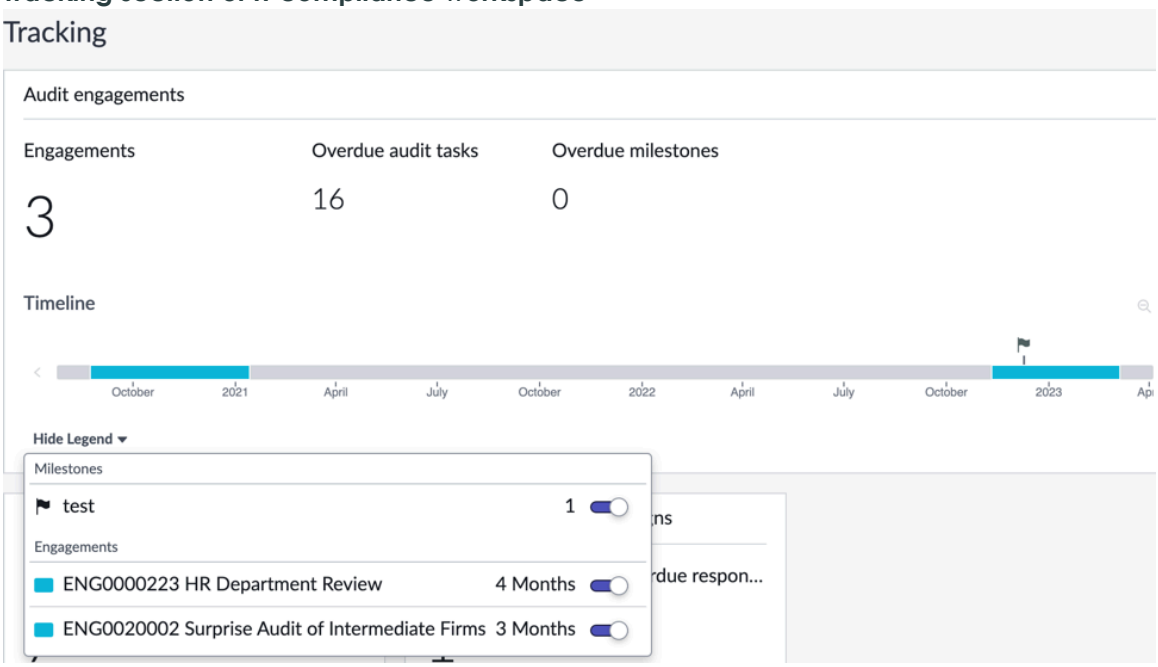
Issues

Provides all issues that are open for the IT compliance manager in the particular functional domain – issues that are open, accepted, the number of exceptions, and the number of expired exceptions. You can click the View issues overview link to take you to the Issues page and filter **IT risk and compliance** data from **All functional domains**.

Tracking

Tracks all the IT-related policies that are in queue for the IT compliance manager's action. The timeline shows the upcoming engagements and the milestones associated to each engagement. It also shows similar reports on exceptions that are active, expiring in seven days, and are at high risk. Similar reports on acknowledgement campaigns that are active and the number of overdue responses are also displayed.

**Tracking section of IT compliance workspace**

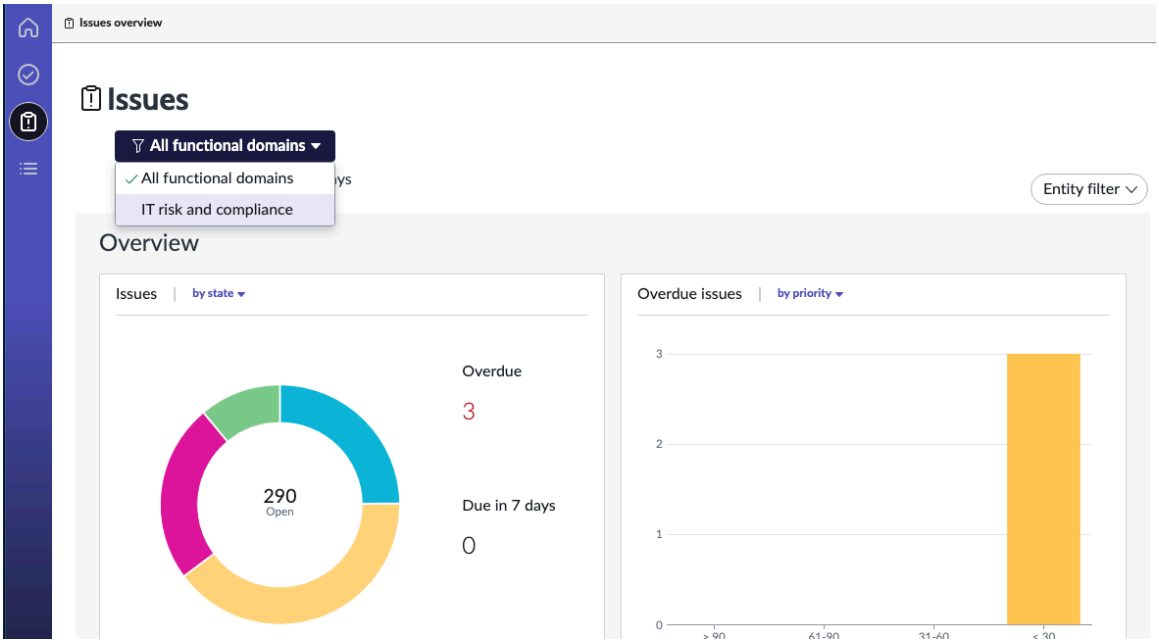



## IT Compliance Issues page

For the IT Compliance workspace, a new functional domain filter is added to filter all IT risk and compliance data from the rest of the GRC audit and compliance data. By default, the filter displays all functional domains. You must select IT risk and compliance to filter the widgets and display IT-related data.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Functional domain filter

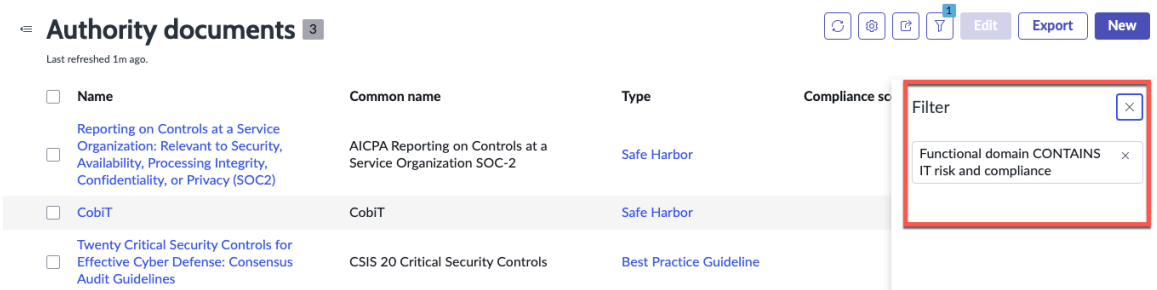



The base condition to filter issues is that the Classification must be Compliance or empty, or in the case where the issue has an m2m association with an engagement, the logged-in user must be one of the three users, such as an auditor, engagement lead, or approver.

## IT Compliance List overview

As you log in as an IT compliance manager, all the data in the List view of the Compliance Workspace are filtered to display those records that fall within the IT risk and compliance functional domain. Therefore, you get to view those records that are related to your user role and complete the IT-related tasks without filtering them manually.

### IT-related records in List view




**Note:** An admin or any user with both corporate compliance manager and IT compliance manager roles can view two list modules with the same name.

## Configuring GRC Compliance Workspace

Configuring the Compliance Workspace requires setting up certain pre-requisite steps.

The following configurations are required to set up the compliance workspace for different users who would be using the workspace:

- To set up the IT Compliance Home page, see Configuring IT compliance workspace.
- For different components installed with GRC: Policy and Compliance Management, see Components installed with Policy and Compliance Management.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- For user roles and access control limitations, see GRC business user role and Assign policy and compliance management roles to your users.
- To set up system properties required in policy and compliance, see Set Policy and Compliance Management properties.
- For mandatory setup steps, see Policy and Compliance mandatory steps.
- To define other properties, rules, templates, and other integrations, see Policy and Compliance enhancement steps.

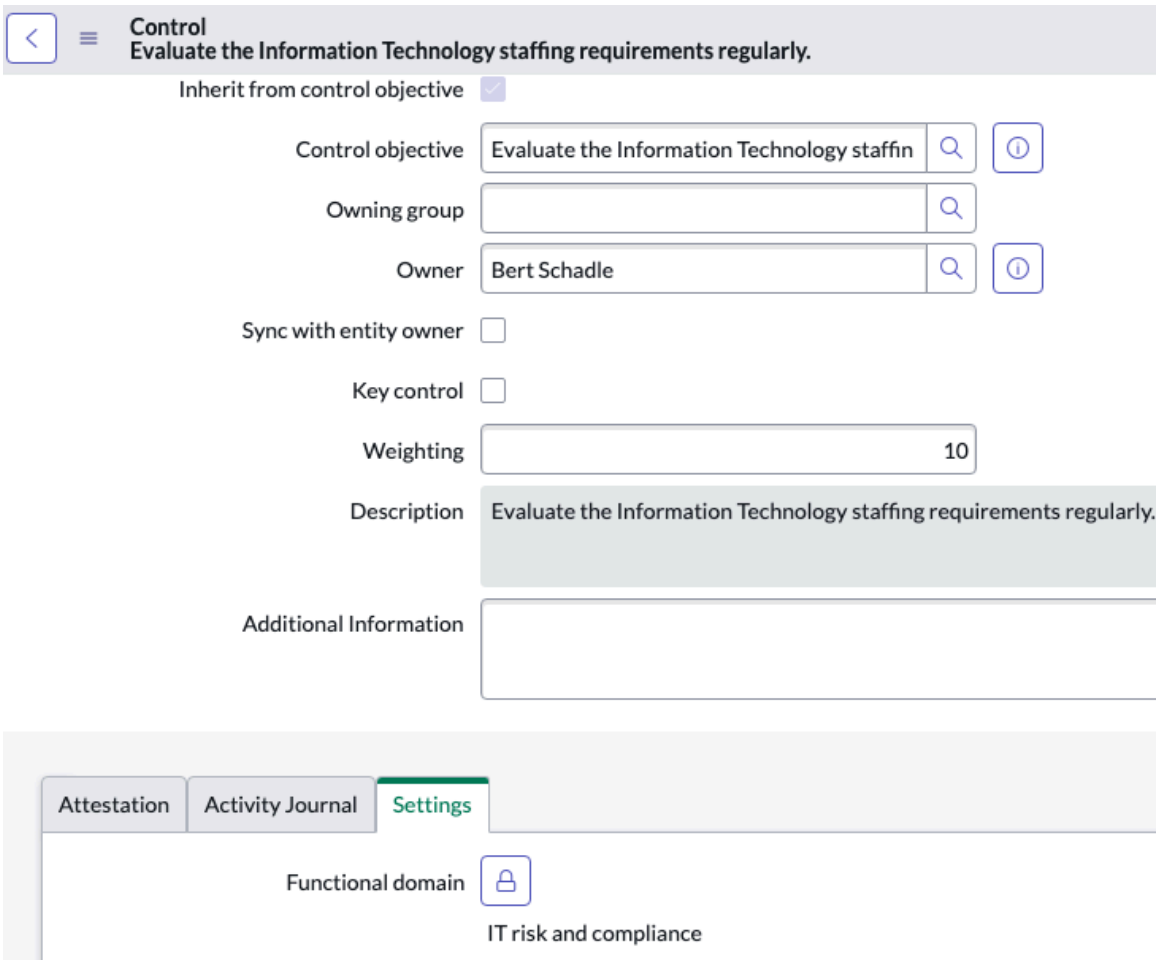
### Configuration steps to filter IT-related data for IT Compliance Home page

There are three distinct steps that must be followed to segregate, associate, and display the IT-related data for the IT compliance manager to view in the IT Compliance Home page.

## GRC data segregation

In all the Compliance Workspace related forms, the **Functional domain** field is added in the **Settings** tab to segregate a particular data and classify it as IT related data. The user must add **IT risk and compliance** as the functional domain.

**Functional domain field**




The **Functional domain** field is available in all GRC compliance and audit workspace related forms such as Entity, Control, Control Objective, Policy, Authority document, Citation, Entity type, Entity class, Issue, Indicator, Indicator template, Acknowledgement campaign, Policy exception, Engagement, Test template, Test plan, Issue triage, Observation, Plan, Audit task, Milestone, Evidence request, and Evidence.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Auto-association of the segregated data

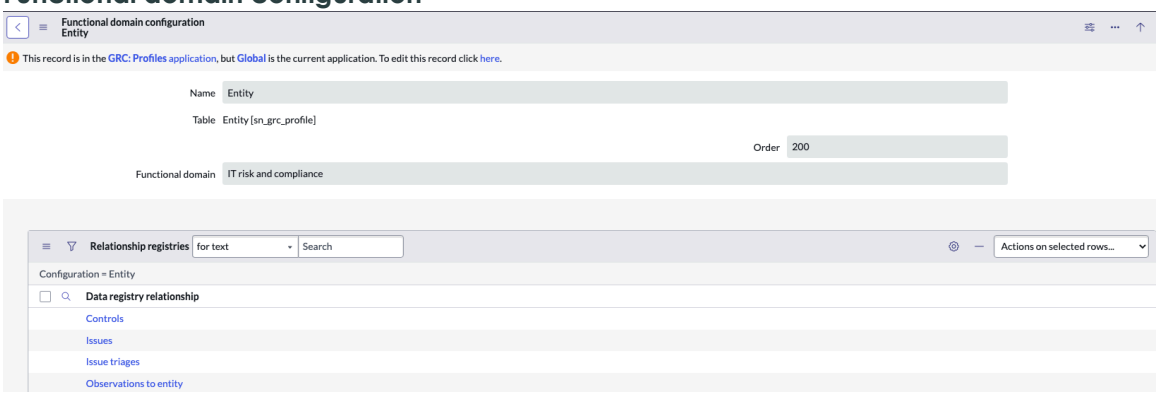
If an audit or compliance object is identified as IT related, then all the related items associated to this object are also identified as IT related. The Functional domain configuration [sn_grc_functional_domain_configuration] table stores the data registry relationship between the parent object and its related child objects within the IT risk and compliance functional domain.

For example, if an entity is classified as IT related entity, then all the controls associated to this entity are auto-associated as IT-related controls. The related child object has all the configurations defined such as the parent table, the child table, and the relationship between the two.

As a system admin, you can define this configuration by navigating to **GRC Administration** > **Functional domains** > **Domain inheritance**. User must manually add the tag, functional domain, in the base forms such as Policy, Authority document, Entity type, Entity class, Entity, Plan, Engagement for auto-tagging the child records. When a parent table is tagged with a particular functional domain, and if the user removes the tag from one of its child records, then the removed tag is not added during auto-association. Similarly, if the user manually adds a tag, then the added tag is not removed during auto-association. The GRC functional domain user action [sn_grc_functional_domain_user_action] table captures and stores all manual actions of the user in the **Functional domain** field of the record that belong to a particular table in the respective functional domain.

For more information on setting up auto-tagging, see the IT Compliance Workspace – Setup and Configurations for auto-tagging [KB1124058] article in the Now Support Knowledge Base.

### Functional domain configuration




A scheduled daily job (GRCObjectsFunctionalDomainChanges) runs and gathers the user's manual actions recorded in the table to read these relationships, auto-associate the child object to IT risk and compliance functional domain, and auto-populate the record in the related item of the parent table.

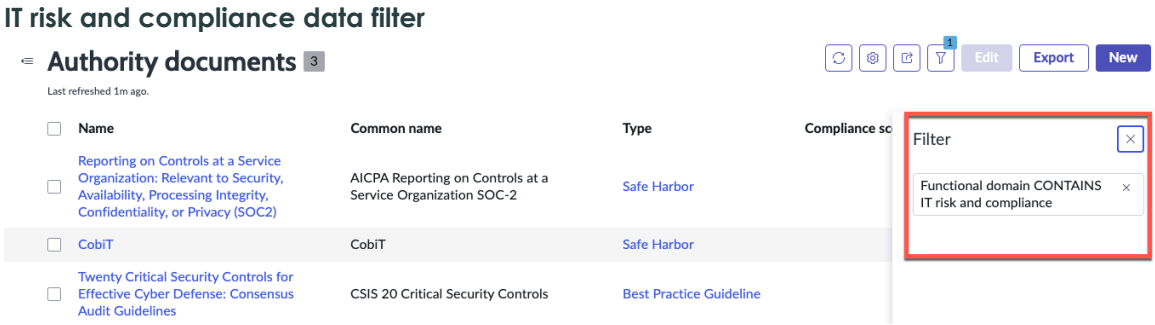
For more information on the tables used for IT compliance workspace, see Components installed with Policy and Compliance Management.

## Display segregated data to IT compliance manager in IT Compliance Home page

The IT compliance manager is the user who can access the IT risk and compliance data in the Compliance Workspace. In the List view of the Compliance Workspace, there is a filter that restricts the display of all audit and compliance data but refines to display only the IT risk and compliance data. The filter uses the Functional domain field in the all the audit and

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

compliance related base forms to filter and display the IT related data in the Compliance Workspace List modules.




**Note:** An admin or any user with both corporate compliance manager and IT compliance manager roles can view two list modules with the same name.

## Using the Compliance Workspace

The Compliance Workspace has a unified tasks page. Based on the user role you can fulfil all your tasks and your team's tasks in the page.

The tasks that appear in the Compliance Workspace are unique to the logged in user and therefore can complete all assigned tasks.

- Use the Tasks page to view the tasks by categories, filter them by various parameters, and track the tasks that you've initiated.
- Use the Issues page to know all about issues.
- The record overview page provides the summary of each record in a single view.
- The contextual pane in the overview page provides contextual information of the record. It provides the record's key information in a hierarchy with attachments, if available.
- Use the 360° view to visualize the record's data relationship within the enterprise, its scores and ratings, and drill down further for more granular information.

### Manage control objectives and policies using the Compliance Workspace

You can use the Compliance Workspace to manage information related to policy approvals, policies, and control objectives.

### Create a policy using the Compliance Workspace

A policy defines an internal practice that processes must follow. You can define policies using the Compliance Workspace as policies, procedures, standards, plans, checklists, frameworks, and templates.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst or sn_compliance_ws.corporate_compliance_manager

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Click the **Create** list and select **Policy** from the **Home** page.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create New Policy form

| Field | Description |
|---|---|
| Name | The name of the policy. |
| Type | List of options:<br>◦ Policy<br>◦ Procedure<br>◦ Standard<br>◦ Plan<br>◦ Checklist<br>◦ Framework<br>◦ Template |
| Parent | The policy containing this policy. If you create a control objective from within a policy, this field is automatically filled. |
| Policy categories | Click the lock icon and select one or more categories for filtering policies. For example, select Vulnerability Response to view policies associated with that application. |
| Description | A general description of the policy. |
| Policy text | A detailed description of the policy. |
| State | The state is a read-only field. Possible choices are:<br>◦ **Draft** In this state, all compliance users can modify the policy and control objectives. All compliance users can click **Request review** button. Enter a message in the Request review pop-up and click **Request** , which sets the state to Review.<br>◦ **Review** In this state, the owner, owning group, and reviewers can modify the policy and control objectives. The owner, owning group, and reviewers click **Request approval**, starting the workflow by sending approvals to the users in the Approvers list. The owner, owning group, and reviewers move the policy back to Draft, by clicking **Back to draft**, as well.<br>◦ **Awaiting approval** In this state, the policy and control objectives are read- only for all. Approvers can approve the policy by updating the approval state in the Approvals related list of the policy form, or by viewing **My Approvals**. If the policy is approved, the policy goes to the **Published** state. Otherwise, it goes back to the **Review** state.<br>◦ **Published** In this state, the policy and control objectives are read-only for all. Admins can click **Retire** which sets the state of the policy to **Retired**<br>◦ **Retired** In this state, the policy is read-only for all. |
| Compliance Score Percentage | The compliance score percentage assigned to this policy. |
| Assignment | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Owning Group | Group that owns the policy. |
| Approvers | The users you want to be included in the approval process. |
| Reviewers | Select the users that you want to be included in the review process. |
| Schedule | |
| Valid from | The date and time for which the policy becomes valid. |
| Valid to | The date and time for which the policy is no longer valid. |
| Knowledge Base | |
| Policy template | The article template to use for the publication of this policy. |
| Policy knowledge base | The knowledge base article related to this policy. |
| Published policy | The KB article number and link where the policy is published. |
| Acknowledgement setup | |
| Audience | Select the default audience responsible for acknowledging this policy. |
| Reference Material URL | Click the lock icon to add the URL for any needed reference materials, such as certification or training materials. |
| Allow users to decline policy | Select this check box to give users the option of declining policy acknowledgements. |
| Allow users to request exception | Select this check box to give users the option of requesting exceptions for policy acknowledgements. |
| Exception Setup | |
| Maximum exception duration (days) | Enter the maximum number of days for which a policy exception can be requested for a given policy. |

4. Click **Save**.
   In the reporting overview page of the policy, you can see the description of the policy, its state, and its status of overall compliance, entities, control objectives, and control. It also gives you the tracking information of policy acknowlegements, policy exceptions, and issues. The non-compliant entities widget also lists all the non-compliant reliant entities, each with its compliance score.
5. Click any of the related lists to provide more information for the policy.
6. From the **Overview** page, click the **Issues** tab.
   You can add existing one or more related issues to the policy that you created. By mapping the existing issues to the policy, you can reduce the count of open issues.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**a.** Click the **Add** button.

**b.** Select a related issue or issues from the Issues pop-up.

**c.** Click **Add**.
The selected issues are added to the policy as related issues and an m2m relationship is created between the policy and the issues in the Issue to Document [sn_grc_m2m_issue_document] table. You can also create an issue for the policy by clicking the **New** button, which takes you to the Create New Issue form.

**d.** To remove an issue that is mapped to the policy, select the issue and click **Remove**.
The remove action only removes the mapping or the association between the policy and the issue in the m2m table and doesn't delete the issue record.

> **Note:** The UI action buttons such as New, Add, Remove aren't available if the policy is in Draft or Retired state. A policy in draft state is considered inactive and becomes active when it moves to Review state.

**7.** To mark the policy ready for review, click **Request review** .

### Manage compliance of a policy from the overview page

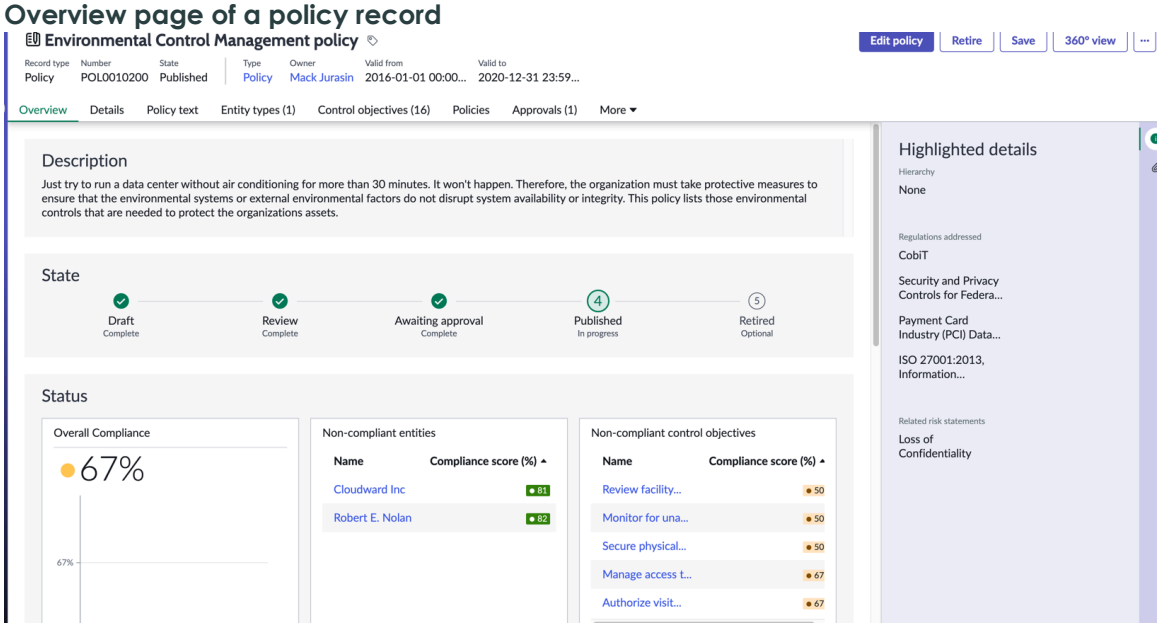
The policy module helps you to create and document all policies. Policies are high-level statements that define what a business should or should not do.

## Overview of a policy

The overview page of a policy record describes the necessity of the policy with respect to the organization's assets. It also gives you the status of the policy, its overall compliance percent, non-compliant entities, and control objectives. It also tracks the open and overdue policy acknowledgements, policy exceptions, and issues.

Select the  icon to know the regulations that the policy has addressed and the related risk statements.

**Overview page of a policy record**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Approve and publish a policy using the Compliance Workspace

When a policy is approved, it is automatically published.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst or sn_compliance_ws.corporate_compliance_manager

#### About this task

Prior to Version 11.0.2 of the GRC: Policy and Compliance Management application, a new knowledge base article overwrote the previous version whenever you made changes to a policy. Starting with Version 11.0.2, when you again approve a policy, a new version of the KB article is created and listed in the **Policy Versions** tab, along with a history of previous versions.

This feature requires that you manually install and activate the Knowledge Management Advanced Installer [com.snc.knowledge_advanced.installer] plugin. For more information, see Activate a plugin.

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Policies**.
2. Open the policy record.
3. Review the policy details.
4. Click the **Request Approval** button.
   Reviewers cannot request approval for a policy. However, the owner of the policy and users with the Corporate compliance manager role can request approval for a policy. When approval is granted, the policy is published and a knowledge base (KB) article is automatically created with the details of the policy.
5. Any time you need to make changes to the policy, you can click **Edit policy** and enter a message in the pop-up, and click **Request Approval**. Add a comment in the pop-up. When approval is granted, a new version of the knowledge base article is created.

   **Note:** As described above, if you activated the Knowledge Management Advanced Installer [com.snc.knowledge_advanced.installer] plugin, a new version of the KB article is created and listed in the **Policy Versions** tab.

   So, if you create links to this policy from the Service Portal or elsewhere, the latest version of the KB article is always displayed.

### Acknowledge a policy using the Compliance Workspace

After a policy has been published, you can create an acknowledgement campaign in the Compliance Workspace to define a group of your employees who must provide an acknowledgement that a particular policy is in compliance. When the campaign has been defined, you can submit the request to the audience.

### Set up a policy acknowledgement campaign using the Compliance Workspace

A policy campaign is the record used to prepare for a policy acknowledgement request. It defines the audience who must provide an acknowledgement that a particular policy is in compliance. A policy campaign is requested in the Compliance Workspace only if the compliance user decides it is needed.

#### Before you begin

Role required: Compliance User

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Policies**.
2. Open the Policy record in the **Published** state you want to acknowledge.
3. Scroll down and click the **Acknowledgement Setup** related list.
4. On the form, fill in the fields.

| Field | Description |
|---|---|
| Audience | Select the employees who are responsible for acknowledging the policy. You define the audience using the Audience module. |
| Reference Material URL | Click the lock icon and add a URL to reference materials for the policy that the audience can review. When you have completed your entry, click the lock icon again. |
| Allow users to decline policy | Select if you want members of the audience to be able to decline the policy. |
| Allow users to request exception | Select if you want to members of the audience to be able to request a policy exception. |

5. Save the record.
6. Scroll down and click the **Acknowledgement Campaigns** related list.
7. Click **New**.

> **Note:** Notice that the majority of the fields are pre-filled with data from the policy record.

8. On the form, fill in the fields.

> **Note:** Only field description that were not previously described are provided here.

| Field | Description |
|---|---|
| Number | An auto-generated record number for the acknowledgement. |
| State | The current state of the acknowledgement campaign. The default state is New. |
| Valid from/to | Select the period of time the acknowledgement is valid. The acknowledgement is valid from the beginning of the **Valid from** date until the end of the **Valid to** date.<br><br>**Note:** The **Valid from** date cannot be prior to the current date. The **Valid to** date cannot be beyond the **Valid to** date defined in the policy. |
| Number of days to respond | The number of days by which members of the audience have to respond. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Short description | A brief description of the policy. |
| **Acknowledgement Details** tab | This tab shows details and requirements from the policy, as well as the **Reference Material URL** defined during acknowledgement setup. |

9. Click **Submit**.
   The acknowledgement request is now ready for you to send to the defined audience.

### Create an audience using the Compliance Workspace

When you set up a policy acknowledgement request in the Compliance Workspace, you must identify an audience responsible for providing the acknowledgement.

#### Before you begin

Role required: sn_compliance_admin or sn_compliance_manager

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policy Acknowledgement** > **Audience**.
2. Click **New**.
3. Enter a name and description for the new audience, and save the record.
4. Use the three tabs to identify members for this audience.

| Option | Description |
|---|---|
| Users | Click **Edit** and add one or more individual users to the audience. |
| Groups | Click **Edit** and add one or more predefined groups of users to the audience. |
| User Filters | Click **New** to define a new filter for audience member inclusion. Click **Edit** to modify an existing user filter. You can save filters for future use. |

5. When the audience has been defined, you can add the users, groups, or user filters to anacknowledgement request.

### Submit an acknowledgement request using the Compliance Workspace

After you have created an acknowledgement campaign using the Compliance Workspace, you can submit the acknowledgement request to the defined audience.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, click the List icon ( ).
3. Navigate to **Policy acknowledgements** > **All campaigns**.
4. Open the Policy Acknowledgement Campaign (PAC) record you want to submit to the defined audience.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Scroll down and click the **Acknowledgement Setup** related list.
6. On the form, fill in the fields.

| Field | Description |
|---|---|
| Audience | Select the employees who are responsible for acknowledging the policy. You define the audience using the Audience module. |
| Reference Material URL | Click the lock icon and add a URL to reference materials for the policy that the audience can review. When you have completed your entry, click the lock icon again. |
| Allow users to decline policy | Select if you want members of the audience to be able to decline the policy. |
| Allow users to request exception | Select if you want to members of the audience to be able to request a policy exception. |

7. Save the record.
8. Scroll down and click the **Acknowledgement Campaigns** related list.
9. Click **New**.

**Note:** The majority of the fields are pre-filled with data from the policy record.

10. On the form, fill in the fields.

**Note:** Only field description that were not previously described are provided here.

| Field | Description |
|---|---|
| Number | An auto-generated record number for the acknowledgement. |
| State | |
| Valid from/to | Select the period of time the acknowledgement is valid. The acknowledgement is valid from the beginning of the **Valid from** date until the end of the **Valid to** date.<br>**Note:** The **Valid to** date cannot be beyond the **Valid to** date defined in the policy. |
| Number of days to respond | The number of days by which members of the audience have to respond. |
| Short description | A brief description of the policy. |
| **Acknowledgement Details** tab | This tab shows details and requirements from the policy, as well as the **Reference Material URL** defined during acknowledgement setup. |

11. Click **Submit**.
12. Click **Request Acknowledgement**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Notice that the following changes occur.

- The state of the acknowledgement campaign changes to **Pending Acknowledgement**.
- Acknowledgement (ACK) records for each member of the audience appear at the bottom of the screen.
- The **Acknowledgement Results** tab shows the progress of the acknowledgement process. That is, it reports the total number of acknowledgements sent, and keeps a running tally of the number and types of responses received (for example, number of accepted, declined, exempted, and so forth).

**Note:** The **Activity** tab shows acknowledgement activities as they happen. The compliance user can click the Work notes check box and post work notes to track changes. The Additional comments box can be used to communicate with the audience.

Also, each member of the audience receives an email notification similar to the following example.

13. As the acknowledgement period elapses, you can monitor the progress of the responses by navigating to **Policy and Compliance** > **Policy Acknowledgement** > **Pending Acknowledgements**.
14. You can also identify any audience members who have exceeded the acknowledgement time line by navigating to **Policy and Compliance** > **Policy Acknowledgement** > **Overdue Acknowledgements**.

### Respond to an acknowledgement request using the Compliance Workspace

After you have been identified as a member of an audience to provide a policy acknowledgement, you must open and review the record in the Compliance Workspace, and then acknowledge it.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst

#### Procedure

1. After you have received a notification that you are required to acknowledge a policy, navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. To provide the acknowledgement, open the record in the **My pending tasks** section of the Tasks page and perform one of the following actions.

   The available options depend on how the acknowledgement request was configured.

   - If the policy is in compliance, click **Accept**.
   - If the policy is not in compliance and the request is configured in such a way that you are allowed to decline the request, click **Decline**.
   - If, for any reason, you do not want to respond, and the request is configured in such a way that you can opt out, click **Request Exception**.

### Retire a policy using the Compliance Workspace

Retiring a policy is part of the policy management process. It can be retired using the Compliance Workspace anytime after being approved and published to the KB.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_compliance_admin or sn_compliance_manager

### Procedure
1. Navigate to **All** > **Policy and Compliance** > **Policies**.
2. Open the Policy record.
3. In the top-right corner, click **Retire**.
   This option is available only for policies in a published state.

## Create a GRC article template

Policy and Compliance managers can use the Compliance Workspace to create templates for policy article publishing.

### Before you begin
Role required: sn_audit.manager

### Procedure
1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Article Templates**.
2. Click **New**.
3. On the form, fill in the fields.

#### Authority Document

| Field | Description |
|---|---|
| Name | Name of the article template. |
| Type | ◦ Script<br>◦ HTML<br>◦ XML |
| Script | The script code. This field depends on the **Type** field. |
| HTML | The HTML code. This field depends on the **Type** field. |
| XML | The XML code. This field depends the **Type** field. |
| Is default | Option to indicate that this template is used as the default template for all KB articles. |

4. Click **Submit**.

## Create a control objective using the Compliance Workspace

A control objective is an objective, direction, or standard that acts as guidance for company interactions and operations. Control objectives can be categorized, classified, and related to policies using the Compliance Workspace.

### Before you begin
Role required: sn_compliance.admin, sn_compliance.manager, sn_compliance.user

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Click the **Create** list and select **Control objective**.
3. On the form, fill in the fields.

### Create New Control Objective form

| Field | Description |
|---|---|
| Name | Name of the control objective. |
| Source | Source of the policy. For example, if the statement is from the a third-party provider, indicate which one. |
| Source ID | Unique identification number used by the source to catalog this authority document. |
| Reference | Unique numerical identifier. |
| Parent | Control objective that is not a child of the current control objective. This is to avoid cyclic parent – child relationship. |
| Compliance Score Percentage | Compliance score percentage calculated for this control objective and its color code:<br>◦ Green: 80 and higher<br>◦ Yellow: 80 to 50<br>◦ Red: below 50 |
| Active | Option that indicates whether a policy is active. |
| Creates controls automatically | Option that indicates that controls are automatically created from the control objective.<br>**Note:** Select this option if the control objective can also serve as the control. |
| Category | List of options:<br>◦ Acquisition or sale of facilities, technology, and services<br>◦ Audits and risk management<br>◦ Compliance and Governance Manual of Style<br>◦ Human Resources management<br>◦ Leadership and high-level objectives<br>◦ Monitoring and measurement<br>◦ Operational management<br>◦ Physical and environmental protection<br>◦ Privacy protection for information and data<br>◦ Records management<br>◦ System hardening through configuration management<br>◦ Systems continuity<br>◦ Systems design, build, and implementation |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Technical security<br>◦ Third party and supply chain oversight<br>◦ Root<br>◦ Deprecated |
| Classification | List of options:<br><br>◦ Preventive<br>◦ Corrective<br>◦ Detective |
| Type | List of options:<br><br>◦ Acquisition/Sale of Assets or Services<br>◦ Actionable Reports or Measurements<br>◦ Audits and Risk Management<br>◦ Behavior<br>◦ Business Processes<br>◦ Communicate<br>◦ Configuration<br>◦ Data and Information Management<br>◦ Duplicate<br>◦ Establish Roles<br>◦ Establish/Maintain Documentation<br>◦ Human Resources Management<br>◦ Investigate<br>◦ IT Impact Zone<br>◦ Log Management<br>◦ Maintenance<br>◦ Monitor and Evaluate Occurrences<br>◦ Physical and Environmental Protection<br>◦ Process or Activity<br>◦ Records Management<br>◦ Systems Continuity<br>◦ Systems Design, Build, and Implementation<br>◦ Technical Security<br>◦ Testing<br>◦ Training |
| Attestation | List of options. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ **GRC Attestation** is chosen by default<br>◦ **Note:** If the user changes the control attestation, the related control objective attestation type is also changed. |
| Issue group rule | Group rule assigned to this control objective. |
| Description | Description of the control objective. |

4. Click **Save**.
   The control objective is created and all related lists are visible.
   - A control is created for every control objective when a policy is associated with an entity.
   - The control attributes default to the same attributes as the related control objective.
5. From the **Overview** page, click the **More** tabs and select **Issues** tab.
   You can add existing one or more related issues to the control objective that you created. By mapping the existing issues to the control objective, you can reduce the count of open issues on the control objective.

   **a.** Click the **Add** button.

   **b.** Select the related issue or issues from the Issues pop-up.

   **c.** Click **Add**.
   The selected issues are added to the control objective as related issues and an m2m relationship is created between the control objective and the issues in issue to control objective [sn_grc_m2m_issue_content] table. You can also create an issue for the control objective by clicking the **New** button.

   **d.** To remove an issue that is mapped to the control objective, select the issue and click **Remove**.
   The remove action only removes the mapping between the control objective and the issue. The action doesn't delete the issue record.

   **Note:** The UI action buttons such as New, Add, Remove aren't available if the control objective is in Retired state.

### What to do next

If you're implementing the Policy and Compliance Management software, return to the Policy and Compliance Management setup checklist and proceed to the next step.

#### Manage a control objective from the overview page

The Overview page of the control objective record gives you the overall details of its compliance status.

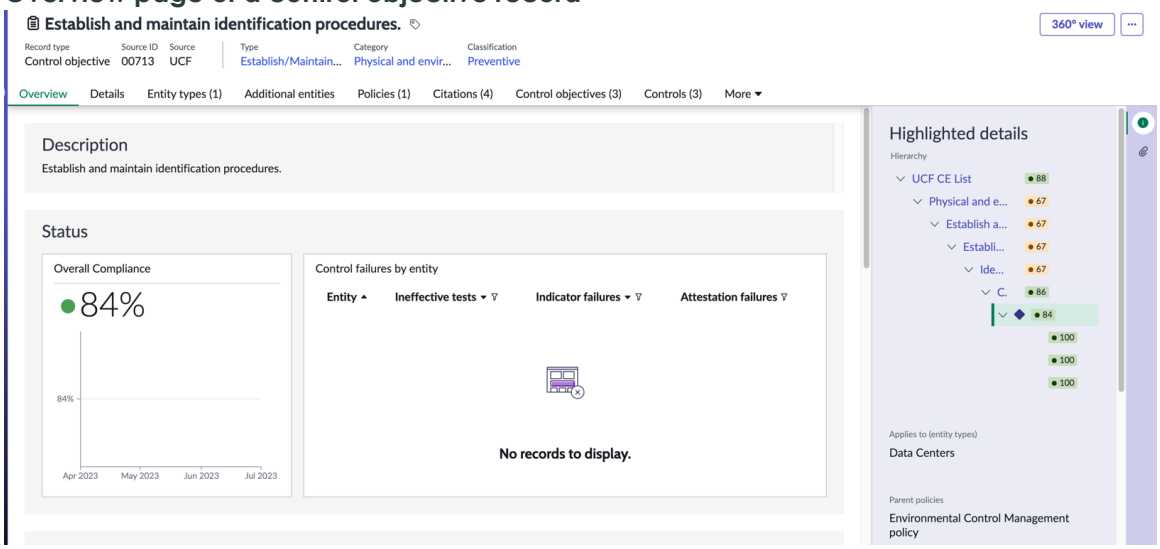
## Overview page of a Control objective record

The control assurance section helps you to know if different attestations are in place, which demonstrates that the control has been implemented correctly. The indicators, in addition to control attestations, help to assess the controls or to monitor their compliance continuously. The ongoing and overdue status of tests conducted on controls is the key determinant by

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

which the organization determines that its policies and authority documents are being followed.

**Overview page of a control objective record**




For more contextual information about the control objective, select the sidebar ( ) icon. For a given control objective record, you can view the hierarchy of mappings back to the authority documents and policies that show why you do the actions indicated in the control objective.

A control objective record has many related lists that come from different applications such as Advanced Risk, GRC Metric, PaCE, and others, which are listed next to the Overview. You can map or associate any of these available related list item with the control objective. For example, if you would like to add an entity type to the control objective, you can navigate to the Entity types related list, select the **Add** button, and map the required entity type.

### Deactivate a control objective using the Compliance Workspace

Using the Compliance Workspace, you can deactivate control objectives that are no longer relevant to their citation or parent control objective.

#### Before you begin

Role required: sn_compliance_admin or sn_compliance_manager

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Control objective**.
2. Open a control objective.
3. In the control objective, clear the check box marked **Active**.
4. Click **Update**.

### Relate a control objective to a policy using the Compliance Workspace

Control objective can be associated to a policy individually when the policy is in the review or draft state. Using the Compliance Workspace, you can choose the policy in the document field on the control objective, or edit the Control Objective related list.

#### Before you begin

Role required: sn_compliance.admin, sn_compliance.manager, sn_compliance.user

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Policies**.
2. Open the policy record.
3. Click **Edit** in the **Control Objectives** related list.
   The slushbucket contains active control objectives with no associated policy selected.
4. Select the control objectives.
5. Click **Save**.
   Those control objective are listed in the **Control Objective** related list.

### What to do next

If you are implementing the Policy and Compliance Management software, return to the Policy and Compliance Management setup checklist and proceed to the next step.

#### Relate a control objective to a citation using the Compliance Workspace

Using the Compliance Workspace, you can map a single control objective to many citations from different authority documents. This function allows you to test a control objective once while complying with many different citations.

### Before you begin

Role required: sn_compliance_admin, sn_compliance_manager

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, click the List icon ( ).
3. Navigate to **Compliance library** > **Citations**.
4. Open a citation record.
5. In the **Control Objectives** related list, click **Add**.
6. Select the control objectives from the Control Objectives pop-up.
7. Click Add.
   The control objectives that you added are related to the citation.

#### Create a citation using the Compliance Workspace

Authority documents, citations, and control objectives are usually downloaded from a third-party provider. However, citations can be created manually from an authority document using the Compliance Workspace. The **Active** option in a citation indicates whether the citation is active or inactive.

### Before you begin

Role required: sn_compliance_admin or sn_compliance_manager

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the lists icon ( ).
3. Select Authority documents in the Compliance library list.
4. Select to open an authority document.
5. In the **Citations** related list, select **New**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. On the form, fill in the fields.

**Citation form**

| Field | Description |
|---|---|
| Name | User-defined name that identifies this citation. |
| Source | Source of the policy. For example, if the statement is from a third-party provider, indicate which one. |
| Source ID | Unique identification number used by the source to catalog this authority document. |
| Reference | Content reference. |
| Type | Type of citation created. Optional field not used for any processing. Use the value in this field in reports or to query for records of a specific type.<br>◦ Core Topic<br>◦ Process<br>◦ Control Objective<br>◦ Control<br>◦ Supporting information |
| Authority document | Name of the parent authority document for this citation. When you create citations from the authority document form, the system completes this field automatically. |
| Active | Option that indicates if a policy is active. A policy is marked active if it is not in the **Draft** or **Retired** state. To deactivate a citation, clear the check box marked **Active**. |
| Parent | References the parent content. |
| Description | Description of the citation. |

7. Select **Save**.
   You can view the description of the citation and monitor the overall compliance, its breakdown, and the non-compliant entities in the different widgets of the **Status** pane in the default **Overview** page. There is also a sidebar, which highlights all the citation record details.

### Create an authority document using the Compliance Workspace

Authority documents manage a process, and citations are created within them to manage the points of the process. For example, the process called Building Security contains a citation for Entry Control.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst, sn_compliance_ws.corporate_compliance_manager, sn_compliance_ws.it_compliance_manager

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the **Create** list and select **Authority document**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. On the form, fill in the fields.

**Create New Authority document form**

| Field | Value |
|---|---|
| Name | Name of the document. |
| Number | Read-only field that is automatically populated with a unique identification number. |
| Source | A non-editable field with the source of the policy. For example, if the statement is from the UCF import, the source is UCF. |
| Source ID | The unique identification number used by the source to catalog this authority document. |
| Version | The unique version number used by the source to identify this authority document. |
| Common name | Abbreviated version of the **Name** field. |
| Category | Category for this authority document. |
| Type | The document type:<br>◦ Audit Guideline<br>◦ Best Practice Guideline<br>◦ Bill or Act<br>◦ Contractual Obligation<br>◦ International or National Standard<br>◦ Not Set<br>◦ Organizational Directive<br>◦ Regulation of Statute<br>◦ Safe Harbor<br>◦ Self-Regulatory Body Requirement<br>◦ Vendor Documentation |
| Valid From | The date and time for which the policy becomes valid. |
| Valid To | The date and time for which the policy is no longer valid. |
| Url | The URL of the stored authority document. |
| Description | More information about the authority document. |

4. Select **Save**.
   The authority document is created and all its related lists are available for your view. By default, the Overview page opens up to display the **Description** of the authority document record and highlights the record details in the sidebar of the page.
5. From the **Overview** page, select the **Issues**.
   You can add existing one or more related issues to the authority document that you created. By mapping the existing issues to the authority document, you can reduce the count of open issues on the document.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select the **Add** button.

b. Select the related issue or issues from the Issues pop-up.

c. Select **Add**.
The selected issues are added to the authority document as related issues. You can also create an issue for the authority document by selecting the **New** button.

d. To remove an issue that is mapped to an authority document, select the issue and click **Remove**.
The remove action only removes the mapping between the authority document and the issue, and doesn't delete the issue record.

**Note:** The UI action buttons such as New, Add, Remove aren't available if the authority document is in Retired state.

### Deactivate an authority document using the Compliance Workspace

The **Active** option in an authority document indicates whether the authority documents have been retired.

#### Before you begin
Role required: sn_compliance.admin or sn_compliance.manager

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance** > **Authority Documents**.
2. Open an authority document.
3. In the authority document, clear the check box marked **Active**.

For Authority documents imported from UCF, users are not allowed to clear the **Active** check box as it is a read-only form.

### Manage policy exceptions and extensions using the Compliance Workspace

Policy exceptions and extensions provide temporary relief for non-compliant controls. The policy exception captures the rationale, comments, and evidence to support the acceptance or rejection of a policy exception request.

Also, you can request an extension to an approved policy exception before the policy exception validity period. The control owner, the compliance manager, and the risk manager may be involved in the policy exception and extension workflow.

### Request a policy exception using the Compliance Workspace

Use the Compliance Workspace to request exceptions for policies, control objectives, or issues by specifying the reason of exception on a particular list of the systems, applications, networks, or entities for which the exception applies. You must also specify the duration for which the exception is required.

#### Before you begin
Role required: sn_grc.business_user, sn_grc.business_user_lite

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

Exceptions provide temporary relief when you are unable to meet compliance requirements due to extraordinary situations. For example, you are unable to meet a control that stipulates all critical OS servers must be patched within 48 hours after the OS vendor releases patches.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Click **Policy exception** in the **Create** list.
3. On the form, fill in the fields.

**Create New Policy Exception form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the policy exception. |
| Requester | Person requesting the policy exception, usually the control owner. |
| Reason | Reason for requesting the policy exception. The requester can change the reason until the policy exception is approved. |
| Short description | Description for the policy exception request. |
| State | State of the policy exception within the approval workflow. |
| Substate | Approval substate of the policy exception within the approval workflow. |
| Priority | Approval priority of this policy exception |
| Justification | Evidence or rationale for the policy exception. |
| Source | |
| Source type | Type of policy exception that you want to create. The options are:<br>◦ Policy: Create a policy exception based on a policy.<br>◦ Control objective: Default is a single control objective on which the policy exception is created.<br>When you select a control objective, the **Impacted controls** tab appears, where you can select controls associated to the control objective.<br>◦ Controls: Option to create a policy exception on multiple controls.<br>Select **Control** to associate multiple controls from different control objectives. This option supports multiple controls objectives for your policy exception, instead of creating multiple policy exceptions that could be applied on multiple controls.<br>◦ Issue: Issue associated with this policy exception. |
| Policy | Policy for which the exception is created. |
| Control objective | Control objective associated with this policy exception. |
| Issue | Issue associated with this policy exception. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Target record | Target record table on which the policy exception is applied. This table is also referenced in the **Policy exception target table** field of the Policy Exception Integration Registry form. |
| Schedule | |
| Valid from | Day on which the policy exception begins. |
| Valid to | Day on which the policy exception ends. Valid to date must be after Valid from date and cannot be a past date. |
| Duration | Number of days between the **Valid from** and **Valid to** dates. |
| Approved extensions | Number of times extensions have been requested so far and have been approved. |
| Remaining extensions | Number of times extensions can be requested in future. `Remaining extensions = Value in the` *`Number of extensions allowed for a policy exception`* `property – Number of Approved extensions`. |
| Created | Date on which the policy exception was requested. |
| Date approved | Date on which the exception was approved. |
| Extension date | Requested extension date, which is after the **Valid to** date. |
| Extension reason | Reason for extension. |
| Original valid to | Date until which the policy exception was originally requested and approved. The original**Valid to** date is populated only when the extension is approved. |
| Assignment | |
| Watch list | Users that are notified when the request is updated. |
| Approval group | Group that has the compliance manager role. If the policy exception reaches Review state you cannot edit the approval group.<br><br>If you don't provide an approval group, then the field defaults to compliance manager. Compliance manager is the default role if the policy exception is raised from any upstream application that is integrated with GRC. For example, if you raise a policy exception for a problem that is related to an incident and that problem is related to GRC. |
| Approver | User from the approval group. If the exception policy moves to the **Analyze** state, then you must select an approver. |
| Risk assessment | |
| Method | Method to assess risk:<br>◦ Select risk rating: Select the risk rating associated to this policy exception.<br>◦ Take risk assessment: Take a risk assessment to calculate the risk rating.<br><br>**Note:** This option is available only when GRC: Advanced Risk plugin is installed. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | Risk assessment can be triggered by clicking the **Assess risk** button on the form. This button is available only when **Take risk assessment** is selected. |
| Risk rating | Risk rating as determined by the risk assessment performed on the policy exception.<br><br>If you had selected **Select risk rating** option in the **Method** field, then you can select a value from the list. If you select **Take risk assessment** option in the **Method** field, then this field is auto-populated with the response provided in risk assessment. |
| Override | Option to override **Risk rating** that was auto-populated based on the responses provided for the risk assessment. This field appears if the **Method** is **Take risk assessment** option. |
| Risk description | Description of the risk as performed by the risk manager during risk assessment. |
| Analysis of risk and impact | Details on the likelihood of this risk occurring and residual impacts of this risk on the policy exception. |
| Risk mitigation plan | Risk mitigation plan for this policy exception. |
| Comments | |
| Work Notes | Work notes can be used by exception reviewers and approvers to share Information about the exception. |
| Additional comments | These comments are used by the reviewer to communicate additional information to the exception requester. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |

**Note:** In versions prior to Version 10.1, the **Risk assessment** related list was called **Business Impact Analysis** and required that the GRC: Risk Management application be activated. Starting in Version 10.1, the dependency on Risk Management has been removed and the associated field names have changed.

**Approved extensions**, **Remaining extensions**, **Date approved**, **Extension date**, **Extension reason**, **Original valid to** fields appear only when you've requested an extension on the policy exception and has been approved by the approver.

With regard to the m2m association of an issue with policy exceptions, there are certain considerations you must know about the values populating in the **Issue** field, **Control objective** field, and in the Impacted control tab:

a. If you select an issue in the **Source type** field, then the **Issue** reference field lists issues that have one or more active controls associated with them. Active controls are the ones in Attest, Review, or Monitor states and not in Draft or Retired states. You can navigate to the Impacted controls tab to view the controls associated to the issue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

b. If the issue is linked to only one control objective, then that linked control objective is populated in the **Control objective** reference field. If the issue is linked to more than one control objective, then no value is populated in the **Control objective** field. Click the **Control objective** reference field to select a control objective.

c. If you didn't select an issue in the **Issue** field, but a control objective is populated in the **Control objective** reference field, then the Issue reference field will list only those issues that are linked to this control objective.

d. As soon as you add an issue in the **Issue** field, then all the controls linked to the issue are added in the Impacted controls tab. However, when you select a control objective in the **Control objective** reference field, then all the controls listed in the Impacted controls tab are replaced with only those controls that are linked to the selected control objective and the issue. Controls can be in any state but not in Draft or Retired state.

e. An impacted control linked to one issue of a policy exception will not be listed for you to add in another policy exception because that control is already listed in the Impacted control tab of the first policy exception. If you add more controls to the issue later, and when you link the issue to the second policy exception, then all the newly added controls will be added as impacted controls but not the one that was already added as an impacted control of the first policy exception.

4. Save the policy exception.
   The Policy exception is in **New** state.
5. Click the **Request approval** button.
   If verification rules are configured, then verification approvals are triggered. After the verification approvals are approved, the policy exception moves to Analyse state.

   After the policy exception is approved and if the **Valid to** date is reached, then the state moves to **Closed** and the substate moves to **Expired**.

   You can also withdraw the policy exception anytime before the policy exception is approved, if it's no longer required, right from the **New** state.

6. To withdraw the policy exception, click the **Cancel Request** button.
   The state moves to **Closed** and the substate to **Canceled**.

### What to do next

As a requester you can request extensions to a policy exception that is in the Approved state more than once. Configure the *Number of extensions allowed for a policy exception* property to request policy extension multiple times.

To set up the property, see Configure the number of extensions allowed for a policy exception.

To request extension, click the **Request extension** button and enter the details in the Request extension pop-up.

Click **Request**. You can see the policy extension details in the Schedule tab of the Policy exception form after the requester has requested for an extension and the policy extension has been approved by the approver.

#### Manage policy exception from the overview page

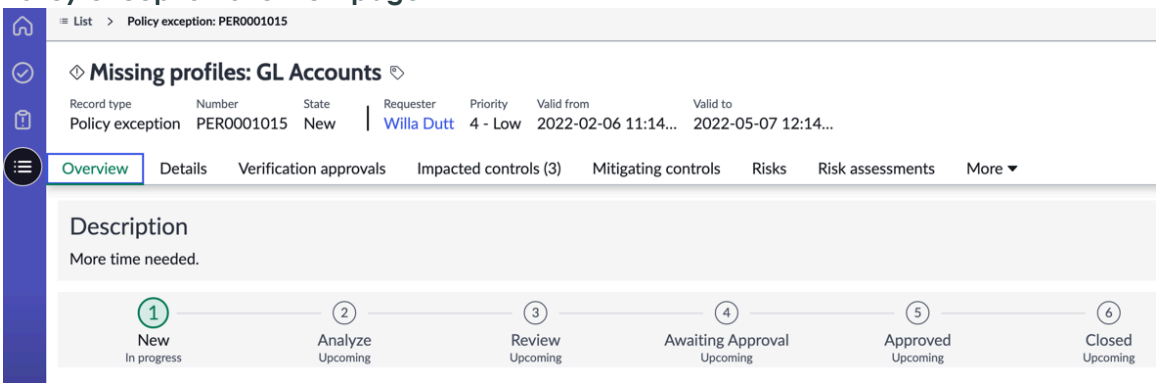
The overview page of the policy exception gives you the overall basic details of the policy exception.

As soon as you save and submit a policy exception, the Overview page opens by default that gives you all the basic details of the policy exception. The header shows the name of the policy exception, the description tells you the justification for the policy exception, and

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the stepper shows the different states the policy exception would pass through before it is finally approved, New state being the default.

**Policy exception overview page**




### Review the policy exception and extension request using the Compliance Workspace

After reviewing a policy exception request using the Compliance Workspace, a compliance manager can accept or reject the request. However, if the compliance manager doesn't have enough information decide, they can request a risk assessment by the risk manager.

#### Before you begin

Role required: sn_compliance.manager

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, click the List icon ( ).
3. Click **All policy exceptions** in the Policy exceptions list.
4. Click the link to the policy exception record in the **Name** column.
5. Perform one of the following actions.

| Option | Action |
|---|---|
| To view or add impacted controls to the policy exception | **a.** Click the Impacted Controls tab.<br>**b.** Click **Add** or **Add All**.<br>**c.** Choose the controls to associate to the policy exception. |
| To view mitigating controls on the policy exception | Click the Mitigating Controls tab. |
| To view or add risks to the policy exception | Click the Risks tab.<br>**Note:** This option is available when Risk Management plugin is also activated. |
| To view or add approvers to the policy exception | Click the Approvers tab. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Action |
| --- | --- |
| To request extension | **a.** Click the **Request extension** button in the **Details** tab.<br>**b.** Select a valid date that is later to the **Valid to** date in the **Extension date** field.<br>**c.** Select a reason from the list in the **Extension reason** field.<br>**d.** Enter relevant information, if any, in the **Additional comments** field.<br>**e.** Click the **Request** button. |

**6.** Perform one of the following actions.

| Option | Action |
| --- | --- |
| To approve the policy exception | Click **Approve**.<br>An email notification is sent to the requester that the PER was approved and goes into effect. |
| To reject the policy exception | Click **Reject**.<br>An email notification is sent to the requester that the PER was rejected and the request is closed. |
| To approve the policy extension | Click **Approve Extension**.<br>An email notification is sent to the requester that the extension request was approved and goes into effect. |
| To reject the policy extension | Click **Reject Extension**.<br>An email notification is sent to the requester that the extension request was rejected and the request is closed. |
| To request a risk assessment on the policy exception | Click **Request Risk Assessment**.<br>An email notification is sent to the risk managers group.<br>**Note:** This option is available when Risk Management is also activated. |
| To request business owner approval | Click **Request Business Owner Approval** . |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Action |
| --- | --- |
| | An email notification is sent to the business owner. |

7. Click **Update**.

### Assess risks of policy exception using advanced risk assessments

Take the advanced risk assessment to evaluate the risk involved with the policy exception.

#### Before you begin

Role required: sn_compliance.manager

GRC: Advanced Risk is the required plugin for the integration with Advanced risk assessment to assess risk using the advanced risk assessment feature.

#### About this task

After the policy exception is submitted, as a compliance manager you can do the risk analysis on the policy exception to evaluate its risk status and determine its approval based on its risk impact on the policy.

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, click the List icon ( ).
3. Click **All policy exceptions** in the Policy exceptions list.
4. Click the link to the policy exception record, for which you want to assess the risk, in the **Name** column.
5. Select the **Take risk assessment** option in the **Method** field of the Risk assessment section. For more information on the risk assessment options, see Risk assessment section.
6. Click **Save**.
7. Click the **Assess risk** button.
   You can assess the risk of a policy exception only when its state is Analyze.
8. Select a risk assessor and an approver in the Specify risk assessor and approver pop-up.
   Any user with compliance user role or risk user role can be a risk assessor or an approver.
9. Click the **Send assessment** button.
   Assessment is sent to the user selected in the pop-up. For more information, see Assess risks and objects on an assessment instance.

   After the assessment is complete, the **Risk rating** field on the policy exception form is auto-populated with the values configured in Policy exception risk rating mapping table.
10. Click the **Details** tab.
    The score calculated based on the risk assessment responses that you provided is mapped with the value in the **Risk rating** field.

### Set up advanced risk assessments for policy exception

Customize the risk assessment methodology by creating your values for each question in risk assessment and calculate your risk rating scores.

#### Before you begin

Role required: sn_compliance.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

If you want to make changes to the Risk Assessment Methodology that is provided by the base system or create a new methodology for policy exception, then the following procedure must be followed after creating or updating the risk assessment methodology for policy exception.

Map the Qualitative Rating Criteria of the risk assessment methodology with the risk rating of the policy exception in the Policy exception risk rating mapping (sn_compliance_policy_exception_risk_rating_mapping) table for the final risk rating score.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Policy exception risk rating mapping**.
2. Enter the corresponding policy exception risk rating value for each risk assessment rating.

   **Note:** The qualitative rating criteria of a residual assessment from a published risk assessment methodology on policy exception table are available options in this field.

3. Click **Save**.
   The score in the risk assessment is converted to the corresponding value in the policy exception risk rating column.

   **Note:** All qualitative rating criteria that are newly configured must have an equivalent mapping with the policy exception risk rating. If the mapping of the Risk assessment rating with the Policy exception risk rating in the Policy exception risk rating mapping table is incorrect, then the **Risk rating** field displays the result as **NONE** along with a message. In this case, you have an option to override the risk rating result of the **Take risk assessment** method and select a value in the **Risk rating** field by selecting the **Override** check box.

   If you are creating a different assessment methodology from the one that is provided by the base system, then you must add the sys_ID of the new methodology in the value field of *sn_risk_advanced.rams_with_extension_points* system property.

#### Manage issues using the Compliance Workspace

Using the Compliance Workspace, you can measure the effectiveness of your company's risk management program by how quickly and completely it identifies and reacts to risk and compliance issues.

#### Manually create GRC issues using the Compliance Workspace

Using the Compliance Workspace, GRC you can manually create issues to document policy, risk, or audit observations, or to accept any GRC problems. You can also identify the source of the issue to help analyze and classify the issues.

### Before you begin

Role required: compliance_admin, compliance_manager, or sn_compliance.user

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, click the List icon ( ).
3. Navigate to **Issues** > **All issues**.
   The list displays all issues. However, the base condition to filter issues is that the Classification must be Compliance or empty, or in the case where the issue has an m2m association with

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

an engagement, the logged-in user must be one of the three users, such as an auditor, engagement lead, or approver.

4. Click **New**.

   For field descriptions of the Create New Issue form, see Compliance workspace issue form.

   **Note:** Starting with Version 12.0.1 of the Policy and Compliance Management application, the minimum role for the **Assigned to** user on the Issues form is GRC Business User [sn_grc.business_user]. The minimum role for the **Issue manager** is GRC User [sn_grc._user].

5. Save the issue record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The tabs enable you to perform various tasks for remediating the issue. You can add policy exceptions and create remediation tasks. You can also view other issues, indicator results, and task SLAs related to the issue.

**Note:** Starting with Version 12.0.1, the **Task SLAs** tab creates and displays SLAs based on the **Due date**. Notifications are sent to the issue owner and issue manager when the issue **Due date** reaches 50%, then %75, then when it breaches. If the **Assigned to** and **Due date** fields aren't empty and the issue isn't in the **New** state, an SLA is created for the issue.

If the due date for the SLA changes, a new SLA is created. The SLA is completed when the issue transitions to **Closed Complete** or **Closed Incomplete**. Also, if the **Due date** or **Assigned to** fields are empty, or the state is New, the SLA is cancelled.

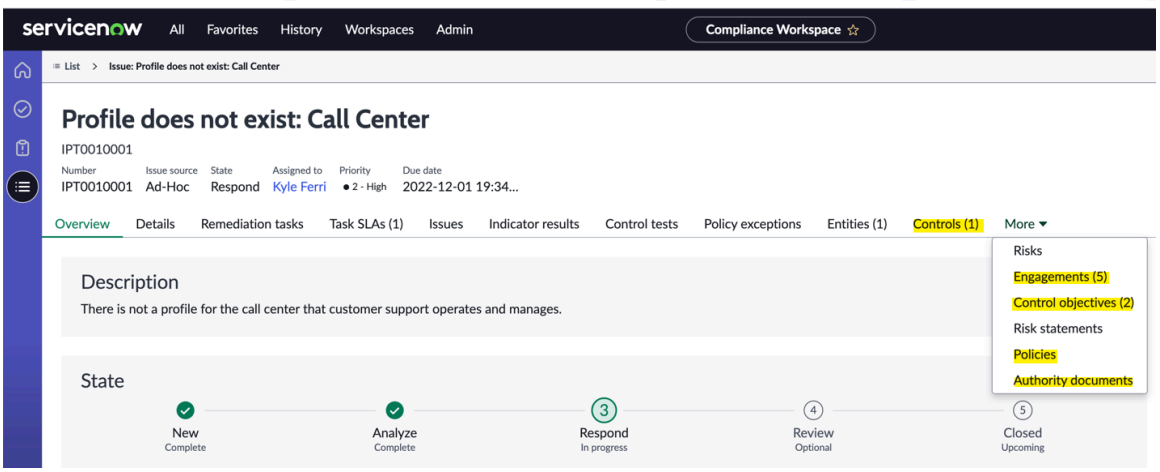
Also starting with Version 12.0.1, remediation tasks can be created by users with the **Assigned to** user and issue manager, as well as any user with the GRC Business User role.

You can navigate to the issue record that you created and use the related lists to.

- Link the issue to multiple records of the same object type such as a control. For example, if there are three controls that monitor Google Cloud, Microsoft Azure cloud, and AWS cloud and there are three different issues raised for them being down, you can link all the three controls to one issue as cloud services is down.
- Link the issue to different objects such as controls, control objectives, policies, and engagements.
- Relate the issue to different type of objects.

**Note:** If the issue is closed, then you cannot create, add, or remove any of the objects from the issue form. You can view the Control, Control objective, Authority document, Policy, Engagement related lists in the Issue Overview page. However, the UI action buttons in each of these related lists such as New, Add, and Remove are inactive.

**Related lists in the Issue form**




The related lists in the issue form for each type of object where the issue can be linked helps to:

- Reduce the number of open related issues existing in an organization.
- Help identify the root cause of the issue and group similar issues.
- Solve one issue, which resolves the related issues.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Compliance Workspace issue form details

Field descriptions to enter on the New Issue form in the Compliance Workspace.

#### Create New Issue form

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name<br><br>**Note:** Until Version 12.0.1, this label was **Short description**. | A name for the issue. |
| Issue source | Source from where the issue was created. This field is auto-populated with one of the following options based on how the issue is created:<br>• Indicator Failure: Issue is created by a failure of the indicator<br>• Risk Assessment: Issue is created in a risk<br>• Risk Event: Issue is created in a risk event<br>• Control Attestation Failure: Issue is created due to a non-compliant control<br>• Control Test Failure: Issue is created when a control is ineffective and the control test is marked as closed and complete<br>• Ad-hoc: Issue is manually created |
| Issue type | Type of issue. Choices are:<br>• Control design effectiveness failure<br>• Control operative effectiveness failure<br>• Control does not meet requirement<br>• Control does not exist<br>• Non-compliance to a regulation<br>• Non-compliance to a policy<br>• Improvement or suggestion to an existing policy<br>• Recommendation for a new policy<br>• Process optimization or improvement<br>• Observation<br>• Data Breach<br>• Fraud<br>• Misstatement<br>• Training<br>• Documentation |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| | • Risk issue<br>• Other |
| Classification | The classification of the issue as a risk, compliance, or audit, based on the issue type. |
| Location | Location where the issue occurred. |
| State | • New<br>• Analyze<br>• Respond<br>• Review<br>• Closed Complete<br>• Closed Incomplete |
| Substate | The substate and applicable details for the substate. |
| Priority | The sequence in which an issue needs to be resolved, based on its impact and urgency:<br>• **1 — Critical**<br>• **2 — High**<br>• **3 — Moderate**<br>• **4 — Low**<br>• **5 — Planning** |
| Issue rating | Starting with Version 12.0.1, the issue manager can assign the issue rating to the issue. Based on the issue rating, the **Due date** under the **Dates** tab is calculated as follows and displayed:<br>• Very high (2 days)<br>• High (4 days)<br>• Moderate (8 days)<br>• Low (10 days)<br>• Very Low (15 days)<br><br>You can manually override the **Due date**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| | **Note:** Users with the sn_grc.manager and sn_grc_advanced.issue_triage_manager role can navigate to **Policy and Compliance** > **Administration** > **Issue rating** and define additional issue ratings.<br><br>When the issue transitions to the **Respond** state, the Issue rating field is read only. |
| Description | Comprehensive description of the issue. |
| Assignment | |
| Assignment group | Group to which this issue has been assigned. Each member receives a notification when activity has occurred on this issue. |
| Assigned to | Member of the group assigned to resolve the issue.<br><br>Starting with Version 12.0.1, the user must have at least the sn_grc.business_user role.<br><br>**Note:** Use the bulb icon to get suggestions on who must the issue be assigned to. The bulb icon only appears if you have the GRC: Predictive Intelligence application activated, the form is saved, the **Assigned to** field is not disabled, and the GRC Property is selected as Similarity Analysis. For more information, see .<br><br>Starting with Version 12.0.1, the assigned-to user receives an email notification when the issue manager requests more information.<br><br>Starting with Version 12.0.1, when an issue transitions to the **Respond** state, an entry in the **Assigned to** field is mandatory. |
| Issue manager group | The group responsible for managing and reviewing the issue.<br><br>Starting with Version 12.0.1, the following enhancements and requirements were introduced: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| | • Members of the issue manager group must have one of the following roles:<br>◦ sn_audit.manager<br>◦ sn_audit.user<br>◦ sn_compliance.manager<br>◦ sn_compliance.user<br>◦ sn_grc.manager<br>◦ sn_grc.user<br>◦ sn_risk.manager<br>◦ sn_risk.user<br>• When an issue transitions to the **Analyze** state, an entry in either the **Issue manager group** or **Issue manager** field is mandatory.<br>• When an issue is assigned to the group, the members receive an email notification. Additionally, the issue manager receives an email notification when the issue transitions to the **Review** state. |
| Issue manager | The user responsible for managing and reviewing the issue.<br><br>Starting with Version 12.0.1, the following enhancements and requirements were introduced:<br>• The issue manager must have at least the sn_grc.user role.<br>• The issue manager receives an email notification when the assigned-to user requests more information.<br>• When an issue transitions to the **Analyze** state, an entry in either this field or **Issue manager** is mandatory.<br>• When an issue transitions to the **Respond** state, an entry in this field is mandatory. |
| Watch list | Users who are on the watch list for the issue. |
| Schedule | |
| Due date | (Starting with Version 12.0.1) This date is auto-populated based on a GRC property. Navigate to **Policy and Compliance** > **Administration** > **GRC Properties**. If the **Auto populate due date based on issue rating** property is set to **Yes**, this field is auto-populated based on the predefined remediation time frame for the issue's risk |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| | rating. Otherwise, you can manually enter a due date.<br><br>When an issue transitions to the **Respond** state, an entry in this field is mandatory. |
| Confirmed date | (Starting with Version 12.0.1) The date when the issue is confirmed. This field is read-only, and displays today's date when the issue is moved from **New** to any of the following states:<br>• **Analyze**<br>• **Review**<br>• **Respond**<br><br>**Note:** If a triage issue is converted to an actual issue, this field displays the date it was converted. |
| Planned start date | Date and time that work on the issue is expected to begin. |
| Planned end date | Date and time that work on the issue is expected to end. |
| Duration | Estimated amount of work time. Calculated using the **Planned state date** and **Planned end date**. |
| Created | The date and time the issue was created. |
| Closed | The date and time the issue was closed. |
| Actual start date | Time when work began on this issue. |
| Actual end date | Time when work on this issue was completed. |
| Actual duration | Amount of work time. Calculated using the **Actual state date** and **Actual end date**. |
| Issue grouping | |
| Parent issue | Parent issue this issue belongs to. |
| Issue group rule | Group rule assigned to this issue. The Issue group rule is used to group similar issues together into a parent issue based on conditions defined in the rule. This allows you to work on similar issues simultaneously and close out the parent issue after all issues are resolved. This closes out all the child issues. |
| Action plan | |
| Recommendation | Resolution actions recommended by the risk, compliance, or audit teams. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| Action Plan | The plan for remediating the issue. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on confidential option, see Confidentiality flag for audit and compliance records. |
| Activity | |
| Work notes (Private) | Click the **Work notes** check box to display the **Work notes** field. Information about how to resolve the issue, or steps already taken to resolve it, if applicable. Work notes are visible to users who are assigned to the issue. Click **Post** to add your work notes to the issue. |
| Additional comments (Customer visible) | Public information about the issue. Click **Post** to add your comments to the issue. |
| Settings | |
| Functional domain | Functional domain for the issue. |
| Details | |
| Control/Risk | The control or risk associated with the issue.<br><br>When the control is associated, the corresponding entity of the control is added to the **Entity** field, and the corresponding control objective is added to the **Control Objective/Risk Statement** field. The control objective and entity are the ones that are linked to this control.<br><br>When the control is associated to the issue form, an m2m record is created in the source [sn_grc_m2m_issue_item] table. Whenever a record is added in the source table, a corresponding record, Issue to Entity is added in the destination [sn_grc_m2m_issue_to_entity] table, and another record Issue to Content is added in the destination [sn_grc_m2m_issue_content] table for the associated entity and control objective of the control. |
| Entity | Related entity. |
| Policy | The policy associated with the issue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| Authority document | The authority document associated with the issue. |
| Control Objective/Risk Statement | The control objective or risk statement related to this issue. |
| Processing activity | |
| Engagement | |
| Engagement | The related engagement. |
| Risk Event | |
| Risk event | The related risk event. |

### Group similar issues under a new parent issue using the Compliance Workspace

When you are creating an issue using the Compliance Workspace, you have the option of grouping the issue with other similar issues.

#### Before you begin

Role required: (per product)

- In Policy and Compliance Management: compliance_admin, compliance_manager, or sn_compliance.user
- In Risk Management: risk_admin, risk_manager, or sn_risk.user
- In Audit Management: audit_admin, audit_manager, audit_admin, or sn_audit.user

#### About this task

Grouping issues under a parent can save you valuable time. For example, assume you have an issue related to patching Windows servers. Since each server is a separate entity, all controls associated with "Windows servers should be patched every Tuesday" will have the same issue. Therefore, the issue can be resolved once for all of the Windows servers by applying the relevant patch one time. So, this feature can be used to group similar issues and resolve them all at the parent level.

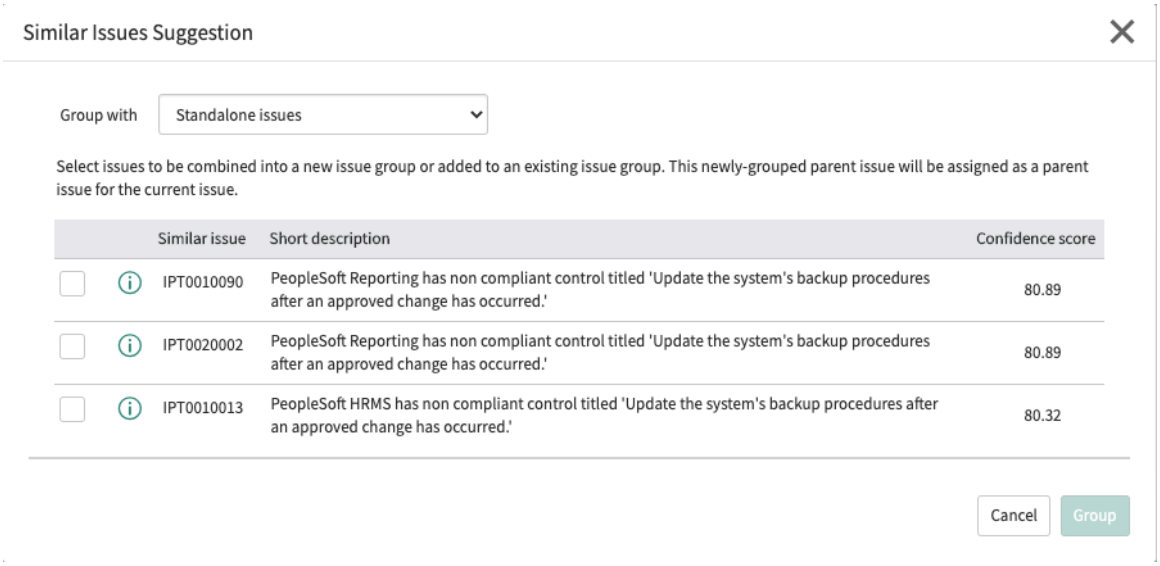
#### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Issues** > **Create New**.
   - **Risk** > **Issues** > **Create New**.
   - **Audit** > **Issues** > **Create New**.
2. On the form, locate the **Parent issue** field.




3. Click the bulb icon ( ) to view similar issues that you may want to assign to this parent issue.

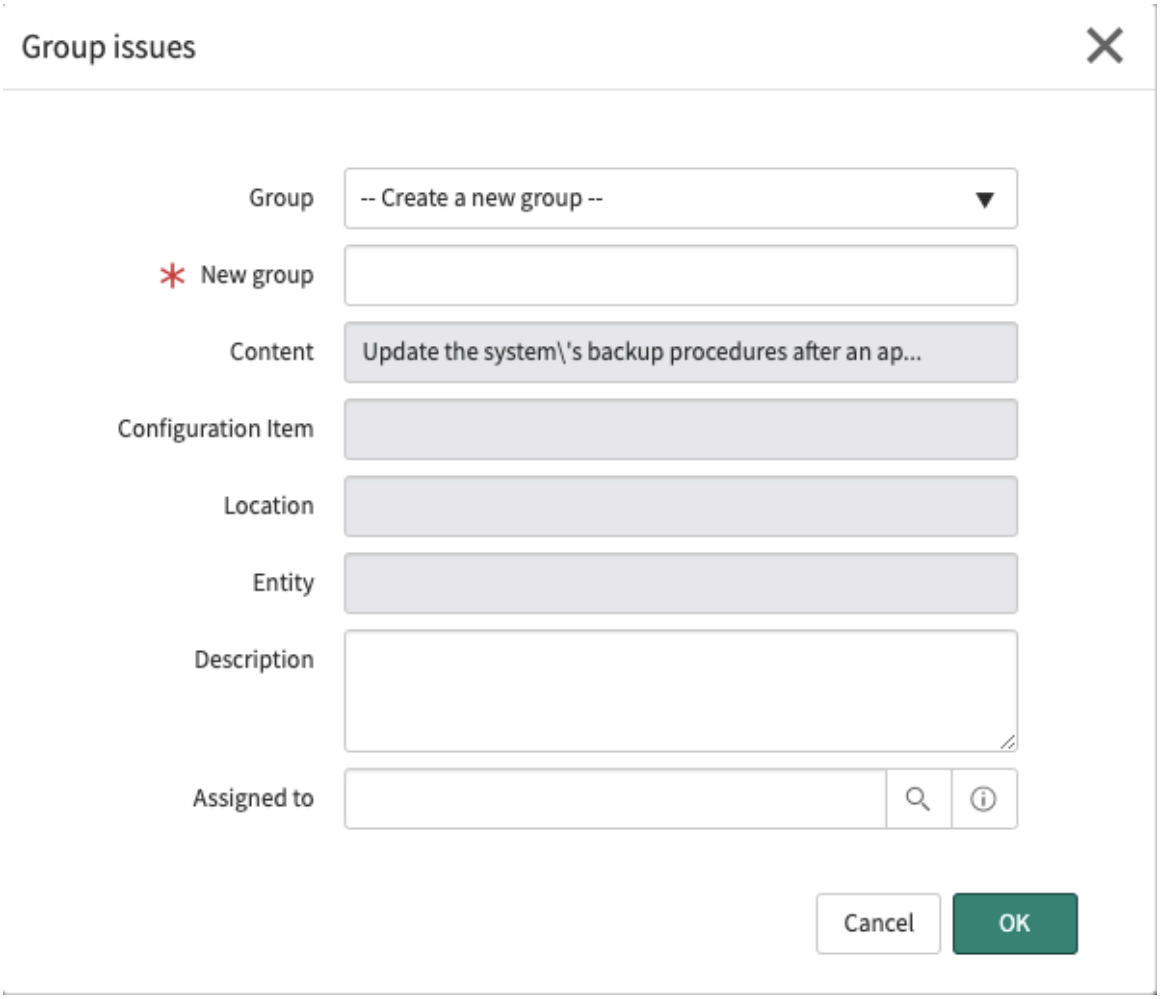
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**Note:** Standalone issues are similar to the current issue, but that are not assigned to a parent issue group. The Confidence score is calculated using a similarity definition included in the GRC: Predictive Intelligence application base system.

4. You can click the Information icon to view details for any similar issues in order to help determine whether they should be grouped with the current issue.
5. Select the similar issues you want to group with the current issue, and click **Group**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




6. On the form, fill in the fields.

**Issue form**

| Field | Description |
|---|---|
| Group | To group the selected issues and assign them to a new group, select **Create a new group**.<br><br>To add the selected issues to an existing group, select the group. |
| New group | This field displays only if you selected **Create a new group**. Type the name of the new group. |
| Description | This field displays only if you selected **Create a new group**. Type a description of the group. |
| Assigned to | This field displays only if you selected **Create a new group**. Select the user to whom the group is assigned. |

7. Click **OK**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The selected issues are added to a new or existing group.

8. You can view the issue in the group by clicking the **Issues** tab.

### Group similar issues under an existing parent issue using the Compliance Workspace

When you are creating an issue using the Compliance Workspace, you have the option of grouping the issue with other similar issues as part of an existing parent issue group.

#### Before you begin

Role required: (per product)

- In Policy and Compliance Management: compliance_admin, compliance_manager, or sn_compliance.user
- In Risk Management: risk_admin, risk_manager, or sn_risk.user
- In Audit Management: audit_admin, audit_manager, audit_admin, or sn_audit.user

#### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Issues** > **Create New**.
   - **Risk** > **Issues** > **Create New**.
   - **Audit** > **Issues** > **Create New**.
2. On the form, locate the **Parent** field.
3. Click the bulb icon ( ) and select **Issues with existing parent** from the **Group with** drop-down list.
4. Click the **Similar issue** you want to group with the current issue.
   The parent issue of the issue you select becomes the parent issue of the current issue.
5. You can view the issue in the group by clicking the **Issues** tab.

### Linking issues to multiple objects using Many-to-many table relationship

Issues can be linked to different types of objects such as risk, entity, control, control objective, engagement, policy, authority document, and others to determine issue impact. Use the many-to-many relationship tables for each of the objects to link similar issues to an object.

**Note:** The Issue record has controls, control objectives, authority documents, policy, and engagements that can be associated with it as related items. However, you must associate the issue and each object as a corresponding m2m record which is stored in the corresponding m2m tables.

For example, issues are configured as a related list in the Controls form and you can link the issue to the control parent object. When you add an issue to a control, a record is created associating the item that is the control with the issue, in the Issue to Control [sn_grc_m2m_issue_item] table.

Viewing the issues related to a control was mainly only for reference. However, you can also link as many issues that are related to the control within the Control form. With this enhancement, you have the ability of:

- visibility of viewing, and consolidating all related issues raised on the control
- determining the impact analysis of all related issues
- reducing the effort in working on duplicate issues and manage issue impact analysis

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

A user with sn_compliance_ws.corporate_compliance_analyst, sn_compliance_ws.corporate_compliance_manager, sn_compliance_ws.it_compliance_manager, or sn_compliance.admin roles can create and delete the records in the many-to-many tables. However, users with these roles cannot update an existing record in the m2m tables. To update a record, you require GRC admin (sn_grc.admin) role.

Many-to-many tables used in Compliance Workspace for creating and deleting the issue to object relationships are:

- sn_grc_m2m_issue_item – Issue to control
- sn_grc_m2m_issue_content – Issue to control objective
- sn_grc_m2m_issue_engagement – Issue to Engagements
- sn_grc_m2m_issue_document – Issue to Policy and Issue to Authority document

For more information, see:

- Tables installed for descriptions of the m2m tables.
- Create GRC issues for the different compliance objects that are linked to the issue.
- Create a control using the Compliance Workspace to link issues to a control.
- Linking automatically generated issues to a control in Many-to-many relationship to know how multiple issues linked to a control are categorized as automatically generated or manually created.
- Create an authority document using the Compliance Workspace to link issues to an authority document.
- Create a control objective using the Compliance Workspace to link issues to a control objective.
- Create an audit engagement in Audit Workspace to link issues to an engagement.
- Create a policy using the Compliance Workspace to link issues to a policy.
- 360° view of compliance objects and issues for a comprehensive and detailed overview of all object data that the issue is linked to in a many-to-many relationship.

### Triage a self-identified issue using the Compliance Workspace

After an issue has been identified and submitted by employees or business users via the Service Portal, the issue triage process begins. The actual problem is identified and assigned to the appropriate owner for prioritization and resolution in the Compliance Workspace.

#### Before you begin

Role required:

- sn_compliance.manager
- sn_compliance.user
- sn_grc_advanced.issue_triage_manager
- sn_grc_advanced.issue_triage_user

#### About this task

Your employees and business users within your company can self-identify an issue and submit it via the ServiceNow® Service Portal. Following submission, a triage issue is automatically created. For more information, see Report self-identified issues via the Service Portal.

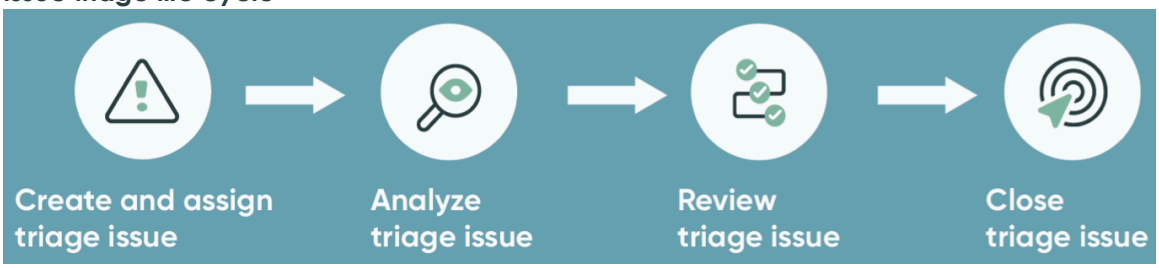
The assigned triage teams identify whether the self-identified issues are actual reported issues, risk events, or observations to be tracked and possibly closed out as noise.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** In the initial release, only self-identified issues are handled by the triage process. In a later release, system-generated issues, such as those caused by indicator or attestation failures, will also be triaged.

The end-to-end flow of the issue triage life cycle is illustrated and described here.

**Issue triage life cycle**




| Stage | Description |
|---|---|
| Create and assign triage issue | An employee identifies an issue related to an entity, control, policy, authority document, process, or risk, and submits a triage request in the ServiceNow Service Portal.<br><br>Based on the type of issue submitted and an issue assignment rule, the issue is assigned to a triage team and a triage owner. |
| Analyze triage issue | The triage team decides whether the issue should be analyzed as an actual issue or risk event, or tracked as a recommendation for a policy or for optimizing a process.<br><br>During analysis, the triage team may request more information from the issue creator. The team may also optionally send the issue to the compliance manager, risk manager, or triage manager with a triage result.<br><br>Possible results include:<br>• Confirmed as a new issue<br>• Confirmed as an existing issue<br>• Confirmed as a risk event<br>• Track as a recommendation<br>• Close as a non-issue/No action required |
| Review triage issue | The Review state is optional. The team may send the issue and result to the compliance manager, risk manager, or triage manager for review. They may also request more information from the triage owner.<br><br>The compliance manager, risk manager, or triage manager decides whether the issue should be confirmed as an issue or risk event, |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Stage | Description |
|---|---|
| | tracked as a recommendation, or closed as a non-issue. |
| Close triage issue | If the issue had been determined to be an actual issue or risk event, those records are created, or the triage issue is added to an existing issue.<br><br>When the triage process is completed, the triage issue is automatically closed. The issue can also be manually closed by the manager and triage team. |

The following user roles are involved in the issue triage process.

### Issue triage personas

| Persona/Role | Description |
|---|---|
| Business user/Employee | Ability to report issue. |
| • Compliance user/manager<br>• Risk user/manager<br>• Triage user/manager | Ability to triage and review issues |
| Issue manager | Ability to manage and review the reportable issue |
| Issue owner | Ability to resolve the reportable issue assigned to them |

**Note:** The triage user/manager and Issue manager roles were introduced in GRC: Policy and Compliance Management version 11.1.0.

## Procedure

1. Navigate to **All** > **Policy and Compliance** > **Issue Triage** > **My Triage Issues** or **Risk** > **Issue Triage** > **My Triage Issues**.
   The list shows triage issues previously created and assigned to you.
2. Click the number of the issue that you want to triage.

   **Note:** The **Classification** field is automatically pre-filled based on the **Issue type** selected. Similarly, an assignment rule called sn_grc_advanced_issue_triage runs and pre-fills the **Triage group**. This rule uses the **Source** and **Classification** to determine the group to which the triage is assigned. Assignment rules also handle issue triages in Risk Management and triages where the **Classification** is set to **Other** (which is initially unknown). For the second use case, you must manually set the **Triage group** to **Risk** or **Compliance**.

3. When you are ready for triage of this issue to begin, select a **Triage owner** and click **Analyze**.
   The assigned Triage owner can open the issue and begin analyzing the issue.
4. During analysis, the triage owner can perform several tasks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Example**
The owner may, for example, decide that the issue is misclassified and can change the **Issue type**. This action could result in the change of Triage group and Triage owner. In this example, the assignment rule runs in the background and the issue is removed from the current owner's queue.

5. The triage owner can also perform the following actions:
   - Click **Request Information** to request additional information from the issue submitter.
   - Click **Request Review** to request a review from the user identified in the **Reviewer** field. That user can open and review the issue by navigating to **Policy and Compliance** > **Issue Triage** > **My Pending Reviews**.
   - Select the **Details** related list to provide additional enrichment to the issue.
6. After it has been determined what action (if any) should be performed on the issue, the triage owner can select a result of the analysis from the **Results** related list.

   **Note:** The options available in the **Result** field depend on the **Issue type** identified for this issue. For example, if you select **Control design effectiveness failure** as the **Issue type**, the following results may be selected.

   If you select a result, such as **Confirmed as a new compliance issue**, which requires more action than simple observation, additional analysis fields appear.

   If the result is **Confirmed as an existing compliance issue**, then an **Existing issue** field appears where you must identify the existing issue that you are referring to.

7. When the issue triage is complete, the triage owner can click **Complete Triage**.

   **Note:** If the issue is out for review, the reviewer can also click **Complete Triage** to complete the triage and create an actual issue.

   The issue triage transitions to the **Closed** state and a link to the issue displays at the top of the screen.
8. The issue can be analyzed using the usual issue management procedures.
   One significant change on the **Issue** form is the addition of an **Issue Triages** related list. Opening the triage record provides the analyst with the details of the triage that resulted in the creation of this issue.

### Remediate an issue using the Compliance Workspace

After an issue has been identified, triaged, and investigated using the Compliance Workspace, you can remediate it.

#### Before you begin
Role required: (per product)

- In Policy and Compliance Management: compliance_admin, compliance_manager, or sn_compliance.user
- In Risk Management: risk_admin, risk_manager, or sn_risk.user
- In Audit Management: audit_admin, audit_manager, audit_admin, or sn_audit.user

#### About this task
Remediating an issue marks an intention to fix the underlying issue causing the control failure or risk exposure. Accepting an issue marks an intention to create an exception for a known control failure or risk. Controls that are **Accepted** remain in a non-compliant state until the

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

control is reassessed. In this way, the issue can be used to document observations during audits.

### Procedure

1. Open the issue you want to remediate.
2. Click the **Remediation Tasks** tab.

   **Note:** You have two options for creating a remediation task:

   - Click **Suggested Remediation Tasks** and click **Copy** to use an existing task as a basis for creating this task. A copy of the selected remediation task is created with certain information from that task copied to the new task. You can manually complete the other fields.
   - Clicking **New** and manually creating the task.

3. On the form, fill in or modify the fields.

**Issue form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Assigned to | Select the user responsible for working this task. |
| Issue | The issue for which this task was created. |
| State | The current state of the task. |
| Priority | Select the priority or sequence this task needs to be resolved, based on its impact and urgency. |
| Watch list | Select users who want to be notified when changes occur. |
| Created/Updated | Displays the date/time when the task was created and updated. |
| Short description | Enter a brief description of the task. This will appear in lists of tasks. |
| Description | Enter a complete description of the task. |
| Notes and Comments | |
| Additional comments | As needed, enter any customer-facing comments related to this task. |
| Work notes | Enter any non-customer-facing notes related to the remediation of the issue. |
| Task Schedule | |
| Planned duration | Estimated amount of work time. Calculated using the **Planned start date** and **Planned end date**. |
| Planned start date | Date and time that work on the task is expected to begin. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Planned end date | Date and time that work on the task is expected to end. |
| Actual duration | Amount of actual work time. Calculated using the **Actual start date** and **Actual end date**. |
| Actual start date | Time when work began on this task. |
| Actual end date | Time when work on this task was completed. |

4. Click **Submit**.

### Manage controls using the Compliance Workspace

Controls are specific implementations of a control objective. Retired controls do not appear in the list. Before defining controls, take time to rationalize, consolidate, and define the important controls in your organization.

## Rationalize your controls

If you upload all your controls in bulk, you are missing the opportunity to refine and streamline your controls set.

- How does this control affect my business objective?
- Is this control actually preventing or detecting risk?
- Is there a different control you can place that better protects your business?
- Is there a control you can put in place that reduces process overhead and improves IT performance while also mitigating risk?
- Can a complicated control be replaced with a simpler more effective control?

As your business changes, and your IT data, processes, and technology improve, replace outdated controls and procedures.

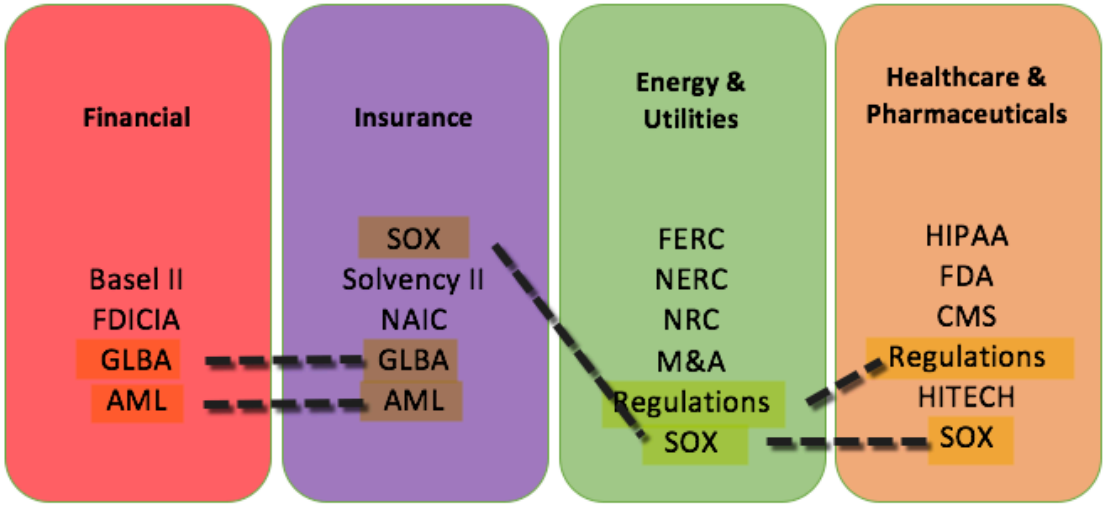
**Note:** When you define controls manually or when you import them from the Unified Compliance Framework (UCF), an entity is associated with the controls. It is a mandatory field on the Control form. If, however, you import controls from a source other than the UCF, you may encounter controls that do not have associated entities. It is important that you return to the Control form and add an entity to the control. Missing entities can cause unreliable results in calculations. Also, if you encounter a control with an entity that has been disabled, the control should be retired.

## Consolidate your controls

Look for opportunities to consolidate controls. Look for common, repeated controls across multiple regulatory authorities of frameworks (for example, SOX and GLBA and AML). Avoid operating a single control multiple times for each regulation, by cross-mapping controls and eliminating the redundant ones. This process establishes a single consolidated set of controls = control framework, performing and preserving the cross mapping of controls is critical for audits.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Industry regulations and requirements overlap**




## Define controls and business rules

The business rules you define up front, establish the GRC configuration settings later. Be prepared to:

- Identify controls and control owners
- Define control tests and expected results
- Establish test and control frequencies
- Identify risks: impact and likelihood
- Prepare attestations, assessments, questionnaires, and required evidence
- Compose likely use-cases (who needs to interact with or view the contents of the GRC system and for what purposes)
- Map authoritative sources to policies, to procedures, to controls, and to risks

### Create a control using the Compliance Workspace

Controls are automatically generated when you associate a policy with an entity type, or an entity type with a control objective, or when an entity is added to a control objective. A control is created for each entity listed in the entity type for the control objective. Controls can also be manually created using the Compliance Workspace.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst, sn_compliance_ws.corporate_compliance_manager, sn_compliance_ws.it_compliance_manager

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Click the **Create** list and select **Control**.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create New Control form

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the control. |
| Entity | Related entity.<br><br>**Note:** If you change the state of the entity to Active from Retired state, then the manually created control on the entity also moves to the Draft state. |
| Status | Control status. Possible choices are:<br><br>◦ **Compliant**<br>◦ **Non-compliant**<br>◦ **Not applicable** |
| Inherit from control objective | Option to indicate whether the control is created through an item generation process. For more information, see Multiple controls for a unique entity–control objective combination. |
| State | Control state. Possible choices are:<br>◦ **Draft** In this state, all compliance users can modify the control. Only available when creating a one-off control. One-off controls are possible but not recommended.<br>◦ **Attest** When the control is created from a control objective, the controls are in this state.<br><br>**Note:** When a control is set back to draft, the attestation is canceled.<br><br>◦ **Review** Controls are automatically moved to review from the attestation phase.<br>◦ **Monitor** In this state, all compliance managers can move the control from review to monitor.<br>◦ **Retired** Compliance managers or administrators can move a control from Monitor to Retired.<br><br>**Note:** When a control is retired:<br>▪ Related indicators do not run<br>▪ Associated attestations are canceled<br>▪ Changes to the associated control objectives do not update the control |
| Key control | Indicator that the control is a key control. |
| Exempt | Mark the control as exempted. |
| Control Objective | Related control objective.<br><br>If you're creating a common control, you must select a control objective. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Enforcement | List of options:<br>◦ Mandated<br>◦ Voluntary |
| Function | Read-only function field. All controls created are **Standard control** by default. When you convert the control to a common control, the value changes to **Common control**. |
| Weighting | Weight used to calculate the control failure factor of a risk. Set the weighting between one and 10. |
| Frequency | List of options:<br>◦ Event Driven<br>◦ Daily<br>◦ Weekly<br>◦ Monthly<br>◦ Quarterly<br>◦ Semi-annually<br>◦ Annually<br>**Note:** For information on the difference between the**Frequency** field for a control and the**Attestation Frequency** field in an entity, see KB0694607. |
| Category | List of options:<br>◦ Acquisition or sale of facilities, technology, and services<br>◦ Audits and risk management<br>◦ Compliance and Governance Manual of Style<br>◦ Human Resources management<br>◦ Leadership and high-level objectives<br>◦ Monitoring and measurement<br>◦ Operational management<br>◦ Physical and environmental protection<br>◦ Privacy protection for information and data<br>◦ Records management<br>◦ System hardening through configuration management<br>◦ Systems continuity<br>◦ Systems design, build, and implementation<br>◦ Technical security<br>◦ Third party and supply chain oversight<br>◦ Root<br>◦ Deprecated |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Type | List of options:<br><br>◦ Acquisition/Sale of Assets or Services<br>◦ Actionable Reports or Measurements<br>◦ Audits and Risk Management<br>◦ Behavior<br>◦ Business Processes<br>◦ Communicate<br>◦ Configuration<br>◦ Data and Information Management<br>◦ Duplicate<br>◦ Establish Roles<br>◦ Establish/Maintain Documentation<br>◦ Human Resources Management<br>◦ Investigate<br>◦ IT Impact Zone<br>◦ Log Management<br>◦ Maintenance<br>◦ Monitor and Evaluate Occurrences<br>◦ Physical and Environmental Protection<br>◦ Process or Activity<br>◦ Records Management<br>◦ Systems Continuity<br>◦ Systems Design, Build, and Implementation<br>◦ Technical Security<br>◦ Testing<br>◦ Training |
| Classification | List of options:<br><br>◦ Preventive<br>◦ Corrective<br>◦ Detective<br>◦ IT Impact Zone |
| Description | Description of the control. |
| Additional Information | Additional information about the control. |
| Assignment | |
| Owning group | Group that owns the policy. |

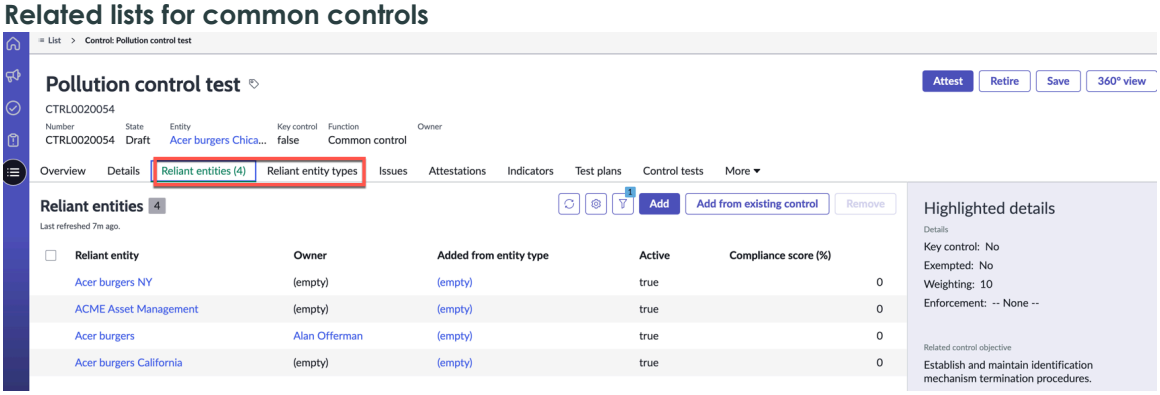
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Owner | User that owns the policy.<br><br>**Note:** The owner is always added as a respondent. The control owner that you select belongs to the owning group. |
| Attestation | |
| Attestation | Select from a list of options.<br><br>◦ Other attestation types can be configured.<br>◦ If this field is populated, then the **Attestation Respondents** field automatically becomes mandatory, and the owner is made the respondent.<br><br>**Note:** If the user changes the attestation type in the control objective, all the related controls are changed also. |
| Attestation respondents | ◦ Users assigned to the attestation of this control.<br>◦ Only a user with the sn_grc.user role can be added as a respondent.<br><br>**Note:** When both the **Attestation** and **Attestation respondents** fields are set, attestations are created when you click **Attest**. |
| Activity Journal | |
| Additional comments | Public information about the control. |

4. Click **Save**.
   The control is created and all related lists are visible.

   If you had created a common control, then there are Reliant entities and Reliant entity types related lists along with other related lists of the control. Use the Reliant entities related list to associate entities to the common control. Or, you can use the Reliant entity types related list to add a group of entities of an entity type instead of associating them one by one.

**Related lists for common controls**




**Note:** For more information on the reliant entity association for a common control, see Convert standard control to common control and add reliant entities.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. From the **Overview** page, click the **Issues**.
   You can add existing one or more related issues to the control that you created. By mapping the existing issues to the control, you can reduce the count of open issues on the document.

   When you add an issue to a control, a record is created associating the item that is the control with the issue, in the Issue to Control [sn_grc_m2m_issue_item] table.

   a. To add an issue to the control, click the **Add** button.

   b. Select the issue or issues related to the control from the Issues pop-up.

   c. Click the **Add** button.
      The selected issues are added to the control as related issues. You can also create an issue for the control by clicking the **New** button.

   d. To remove an issue that is already added to the control, select the issue and click **Remove**.
      The associated record mapping between the issue and control is removed from the Issue to Item table.

      **Note:** The UI action buttons such as New, Add, Remove aren't available if the control is in Retired state.

#### Linking automatically generated issues to a control in Many-to-many relationship

You can link an automatically generated issue that belongs to a different control as a related issue to a control. The **Originator** flag helps you to differentiate those control issues that were automatically generated from the controls that were manually created.

## Manually created and automatically generated issues

**Note:** You can identify the origin of an issue whether it was automatically generated or manually created after you link the issue from one control to another only in a control form.

You can create an issue manually for a control when you click the **New** button in the Issues related list of a Control form. For manually created issues, see Manually create GRC issues.

However, issues are also automatically generated when there are:

Control test failure

If there's a control test which is linked to a control and when one of the test is marked ineffective and closed, then the control becomes non-compliant. As a result, an issue is automatically generated. Control tests can be design test or operational test which can be marked ineffective and the tests can be common across all controls.

Control attestation failure

When the user who is an attestation respondent of a control rejects the control, then the status of the control becomes non-compliant and an issue is automatically generated.

Control indicator failure

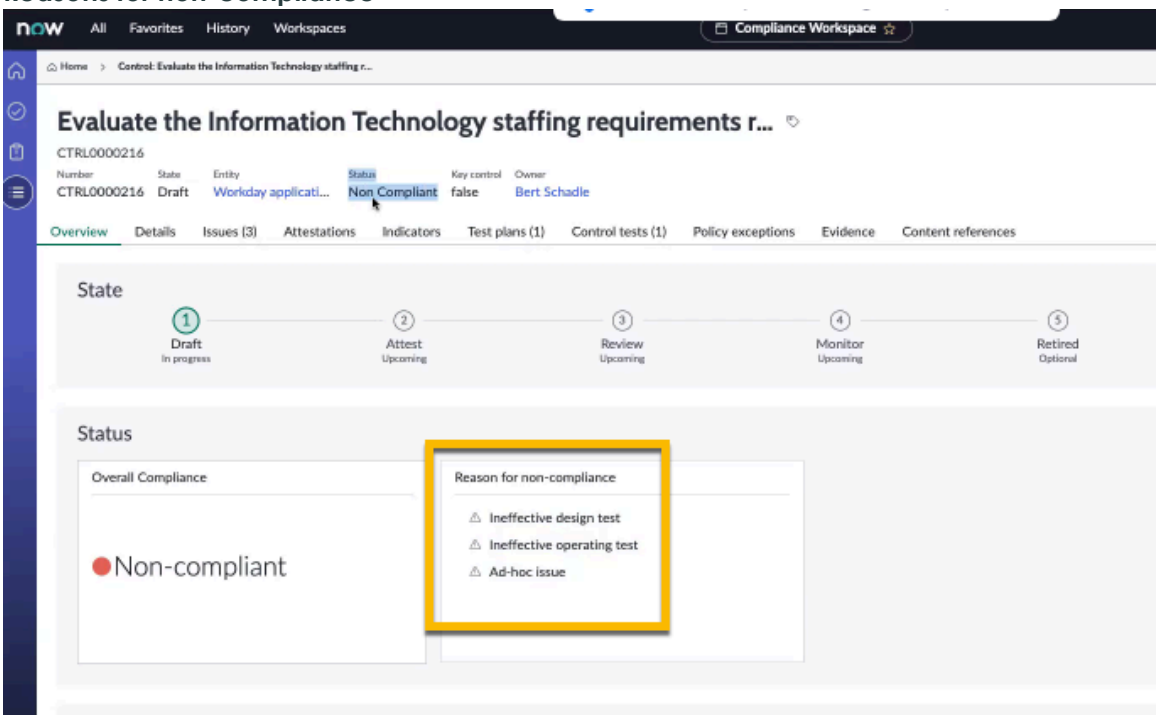
Similarly, when a control indicator fails, the control becomes non-compliant and an issue is automatically generated.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The source of the issue generation for one or more of the three failures can be tracked with the tags in the **Issue source** field of the Issue details. If there is a control test failure, the **Issue source** field is updated with a tag, **Control Test Failure**. If the issue was created manually, then the Issue source tag is **Ad-Hoc**.

When a control's status moves to non-complaint, all the reasons for non-compliancy are pulled from the **Issue source** field and displayed as **Reasons for non-compliance** in the Status widget of the control's Overview page.

**Reasons for non-compliance**




## Handling more than one automatically generated issue while linking to a control

You can add an automatically generated issue that belongs to another control, to a control in an m2m relationship using the **Add** button. However, adding an automatically generated issue from another control to a control with an existing automatically generated issue conflicts the source of the issue generation. To track the source of issue generation, a back-end flag, **Originator**, is used. It is a true or false flag and is false, by default. Originator is flagged true or false, if:

- An automated issue of another control is associated to the current control, then the **Originator** is false.
- It is a manual issue of the current control, then the **Originator** is false.
- It is an automated issue of current control then the **Originator** is true.

1. When there is an issue that exists with Originator as true, and if a control failure happens, the **Issue source** field of the issue is updated with the source of the issue. For example, there's an issue with originator as true already present and the issue source is Control test failure. If another control failure happens, such as control attestation failure, then the Issue source is updated with two tags, namely Control test failure and Control attestation failure.
2. When there is no issue present with Originator as true, and if one of the three control failures happens a new automated issue with originator as true is created. For example, if there's a

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

control attestation failure for a particular control that has no issue linked to the control with the originator as true, then a new automated issue with Issue source as control attestation failure is created and the originator is true.

## Data migration

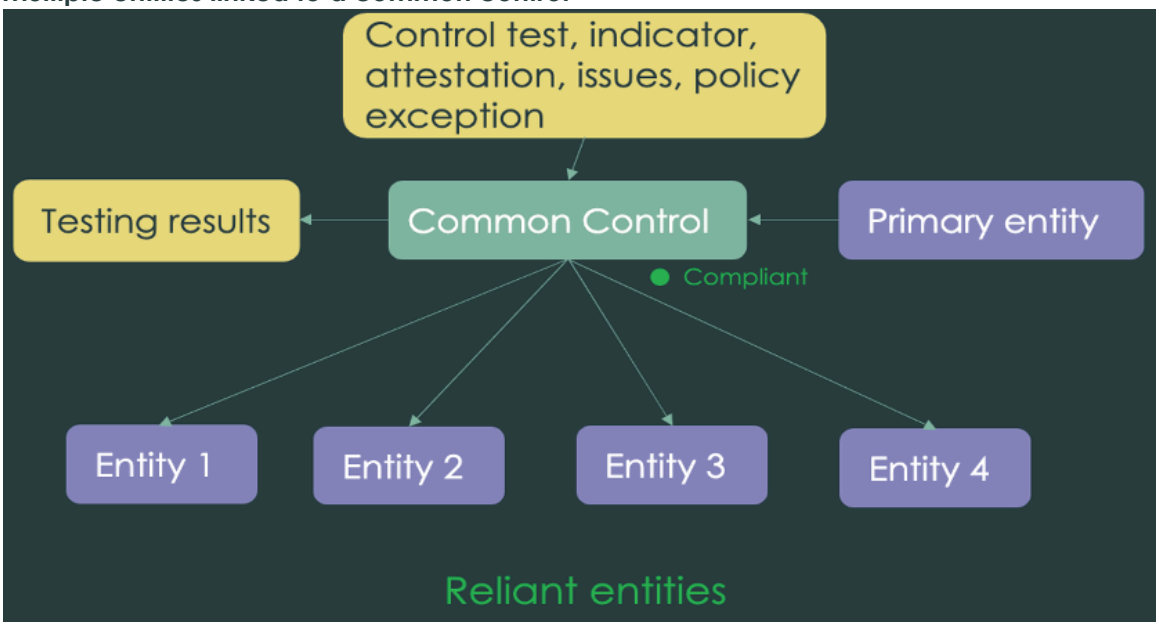
The logic behind flagging an issue as automatically generated or manually created with the Originator flag is handled automatically when you install the latest plugin. For all automated issues linked to existing controls, the originator flag is true in the m2m records between the control and the issue.

### Testing common control and implementing results on multiple reliant entities

Instead of generating controls for individual entities and testing each entity separately with an individual control, you can use a common control and associate a primary entity to it.

Test the common control for control tests, indicators, attestations, issues, and policy exceptions. Use the test results that are inheritable and implement them on all the reliant entities associated to the common control.

**Multiple entities linked to a common control**




Using common controls gives you the ability to:

- Mark a control as common and associate reliant entities to it.
- Associate entities of existing controls as reliant entities to a common control.
- Save time and effort in testing. The result of the common control tests can be inherited by other reliant entities, especially when a new system is deployed and pre-validation audits are conducted within an organization or environment.
- Reduce redundancy of workforce in documenting test results.

Requirements and use case:

- Create a control and convert a control to common.
- Associate reliant entities to a common control to inherit test results.
- Associate entity types to a common control.
- Test the common control once and apply results to multiple entities.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Can convert a common control back to standard.
- Avoid voluminous increase in controls.

For more information, see:

- Tables installed for descriptions of the common item m2m tables.
- Control form changes with respect to common controls.
- Convert standard control to common control to add reliant entities.
- Action handler components for common controls.
- Operational changes in item generation of common controls.
- Impact of common control on compliance score calculation.

### Convert standard control to common control and add reliant entities

Mark a control as common and associate reliant entities to it. Test the common control tied to the primary entity. The reliant entities inherit the results of the common control.

#### Before you begin

Role required: sn_compliance_ws.corporate_compliance_manager, sn_compliance_ws.corporate_compliance_analyst

#### About this task

All existing controls are termed as standard controls. You can convert a standard control to common and reverse its function as standard if you so require. However, by default all controls whether existing or created are standard.

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, click the List icon ( ).
3. Navigate to **Compliance library** > **All controls**.
   You can either create a control by clicking the **New** button or select one of the existing standard controls from the All controls list and convert it to a common control. Either way, the control is standard, by default, and you must convert it to common to add reliant entities.

   **Note:** Before you convert a control from standard to common, ensure that you select a value in the **Control objective** field, and save the form details. Control objective is required for a common control as there are validations to ensure that the common control does not have the same Name, Entity (primary or reliant), and Control objective combination as any other control.

4. Click the More Actions on the top right.
5. Select the **Convert to common** list UI action.
   The **Convert to common** UI action appears only when the control is in the initial states such as **Draft** or **Attest**. When the control progresses beyond these states, then it can neither be converted to common nor reverted as standard control. **Convert to standard** UI action does not appear when the control is common and in the **Review** state.

   When a control is common, its **Source** field is Entity. When the control is converted back to standard, the entity source is removed if it was added when the control was converted to common. When a common control is converted to standard control, the entity type and reliant entity type associations are deleted.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Click **Okay**.

   **Note:** The **Function** field changes from Standard control to Common control. Also, the Reliant entities and Reliant entity types related lists appear on the control form to help you add the reliant entities.

7. To add reliant entities, select the Reliant entities related list.

   a. Click the **Add** button.

   b. Select the entities in the Entities pop-up and click **Add**.
   The message confirms that the reliant entities are added successfully to the common control. The association of the entity as reliant to the common control creates a record in the Item to entity [sn_grc_m2m_item_entity] table.

   If you have an entity type with entities, then you can select the entity type to add the bulk of entities instead of selecting them one by one.

   c. To pick out a primary entity and associate it as a reliant entity, click the **Add from existing control** button.
   This action enables you to:

   - retire that existing control
   - associate the entities of that control as reliant entities

   You can add up to 15 entities at a time by this option. When you select the entities and click **Add**, not all existing entities are added. All of the entities may be added, some of them may be added, or sometimes none of them is added. For reasons as to why the entities are skipped from being added and their controls are not retired, see the GRC Common control inheritance [KB1221601] article in the Now Support Knowledge Base.

   **Note:** You must log in to Now Support to view the articles.

   When you select the **Continue to add** button in the pop-up, the existing control is retired and its associated entity is added as reliant entity. The control is treated as manually retired control.

   d. To remove a reliant entity, select the reliant entity and click **Remove**.

8. To add entity types, select the Reliant entity types related list.

   a. Click the **Add** button.

   b. Select the entity type in the Reliant entity types pop-up and click **Add**.

   The downstream action of associating entity types to a common control creates an upstream action of associating entities to the common control. All the entities that are added as part of the entity type are also listed in the Related entities related list. **Added from entity type** column lists the source of the entity type.

   The association of the entity type as reliant to the common control creates a record in the Item to entity type [sn_grc_m2m_item_entity_type] table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** For more information on the m2m tables that store the records of entity and common control association, see Tables installed with Policy and Compliance Management.

The advantage of using Reliant entity types is that even if you update the entity type later by adding more entities to it, after it is associated to a common control, then those added entities get automatically associated as reliant entities.

c. To remove a reliant entity type, select the record and click **Remove**.

9. To add a risk to the control, select the Risks related list and click the **Add from reliant entities** button.
   Based on the reliant entities' association with risks, you can associate the common control with risks. For more information, see Common controls in Risk Management.
10. To view the reliant entities associated to the control, click the **360° view** button from the control record.
    The primary entity and the list of all reliant entities are displayed in a distinctive visualization.

**Result**
Associating reliant entities to a common control has an impact on compliance scoring.

### Impact of common control on compliance score calculation

Whenever an entity is associated to a common control and termed as a reliant entity, there is an impact on the compliance score of the entity on account of the common control test results.

All active, associated common controls contribute to the compliance score as any other control that exists.

Whenever a control changes its compliance status or weightage, the compliance score for the entities is recalculated. Similarly, in the case of a common control, the compliance score for reliant entities is recalculated as well.

All primary actions trigger recalculation of compliance score. When reliant entities are added or removed using the Add or Remove UI action in the Reliant entities related list as an upstream action, the compliance score for that particular reliant entity is recalculated. It is also recalculated when you retire a common control or convert a common control to standard control. Controls that are either compliant or non-compliant contribute to the compliance score calculation of an entity.

For more information, see the Compliance score calculations in GRC [KB1222566] article in the Now Support Knowledge Base.

**Note:** You must log in to Now Support to view the articles.

### Entity enhancements to support common controls

Learn about the entity enhancements of the downstream inherited controls in the GRC application. For example, you can see information about the downstream inherited controls by looking at the entity record page. You can also see a summary of the downstream inherited controls by using a widget that is available on the entity overview page.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Overview

With the Entity form, you can see the common controls that the current entity or its downstream entities rely on. In the Downstream inherited controls related list, use the **Add** and **Remove** buttons to update the associations of the common controls.

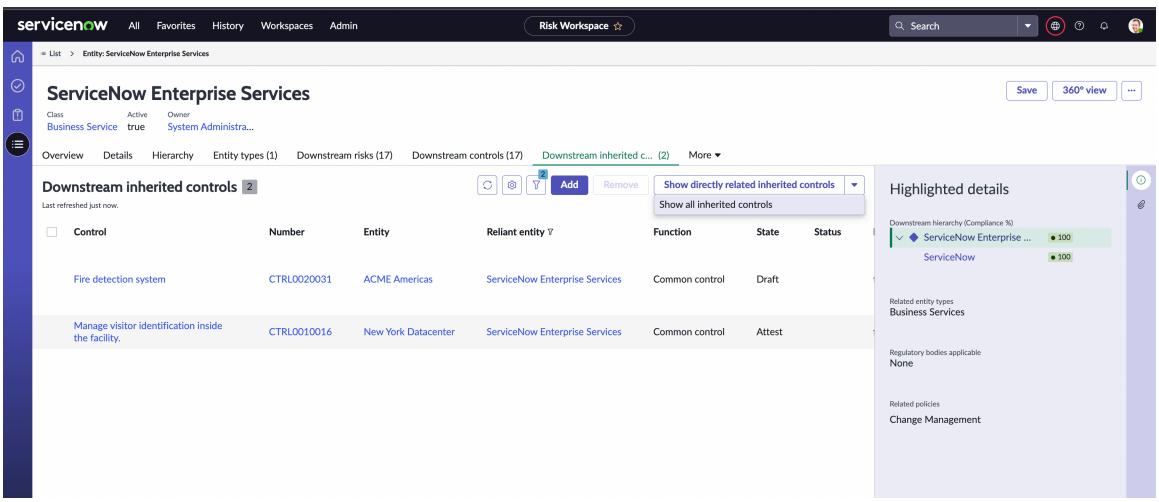
You can also see the common controls that the current entity relies on by using the **Show directly related inherited controls** button and the **Show all inherited controls** button. These buttons display the common controls that the downstream entities are reliant on.

To learn more about the common controls, see Common controls in risk management.

The Downstream Controls related list also displays the common controls that the current entity or its downstream entities use to implement the common controls. By using the Function column in the form, you can differentiate between the standard and common controls. The following example shows the downstream inherited controls.

**Note:** You can add or remove the reliant entity association with the common controls in Workspaces only.

### Downstream inherited controls




In the downstream inherited controls related list, you can see the information about the control, entity, and its reliant entity. The control is implemented by the entity that is listed. The same control is inherited by the reliant entity.

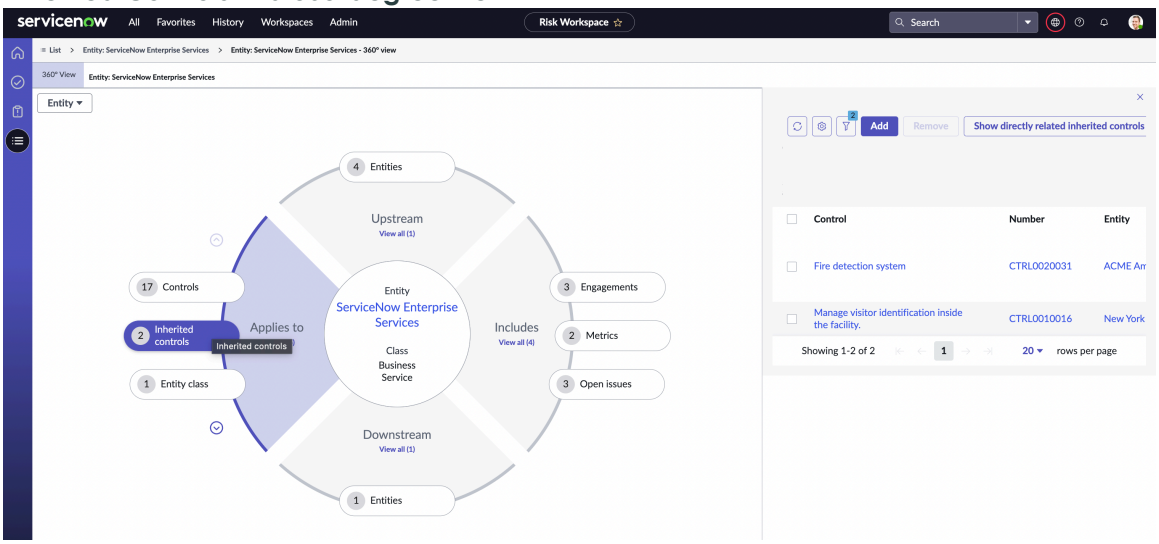
## 360-degree view

The 360-degree view of the entity shows the controls and the inherited controls.

The following example shows that the 360-degree view of the Enterprise Services entity has two inherited controls.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Inherited Controls in a 360-degree view




## Group assessments for similar assessments in the Tasks page

Provide response to similar assessments by grouping the assessments based on metric type, and additionally the same entity, control objective, or category in the Tasks page of the Compliance Workspace.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_manager or sn_compliance_ws.corporate_compliance_analyst

### About this task

In Configurable Workspace, you can only group control attestations, and not risk assessments, vendor assessments, or privacy assessments. Such assessments and those assessments that can't be grouped by the selected **Group by** criterion are marked as invalid and are displayed in the **Group previews** of the Group assessment pop-up, with a link to view such assessments.

### Procedure

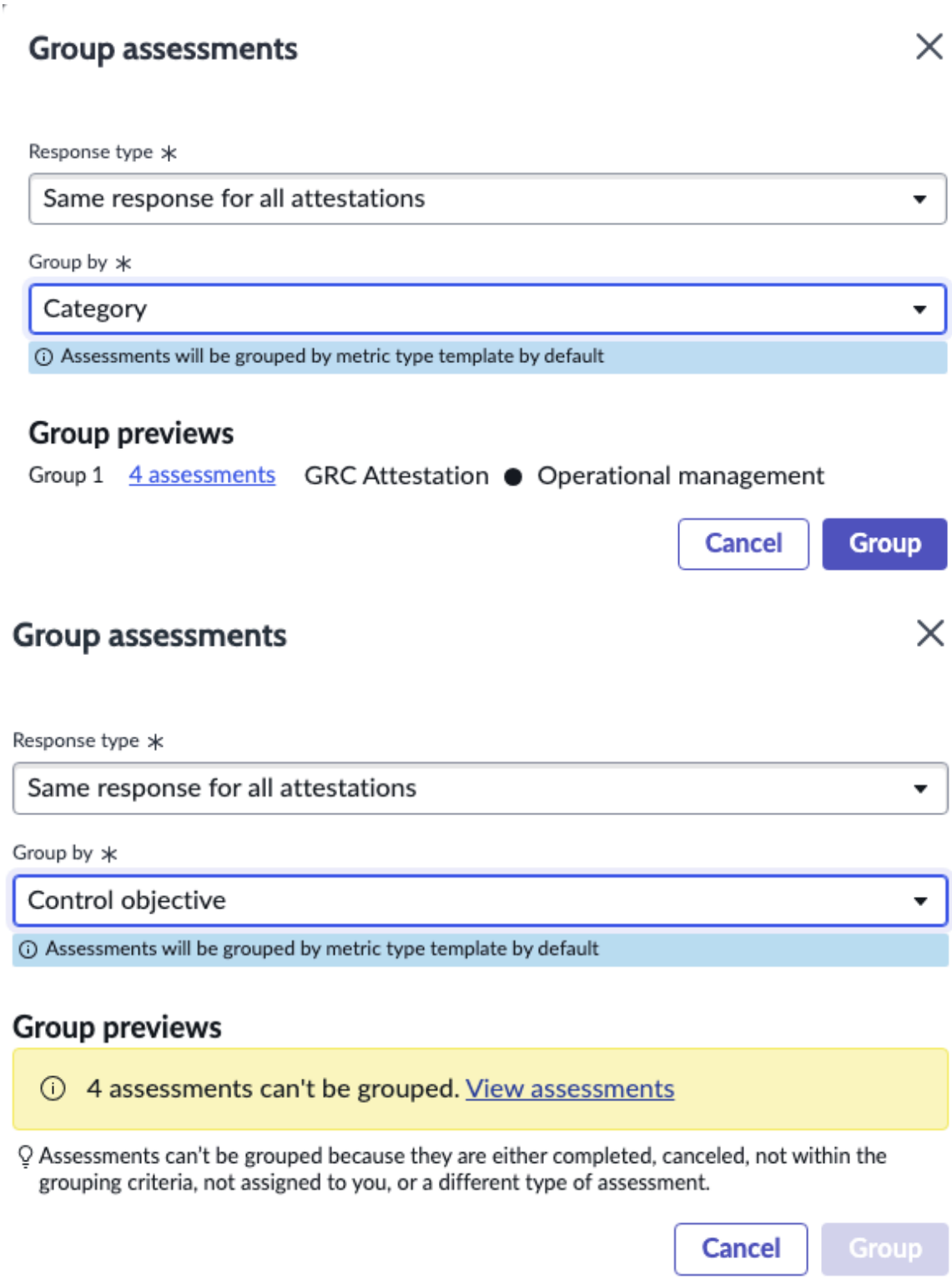
1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. Select the Tasks icon on the left pane.
3. Select the attestation records in the My pending tasks tab that you'd like to group.

   **Note:** You must select at least two and can select up to a maximum of 13 assessment records for grouping.

4. Select the **Group assessments** button.
5. Select a **Response type** in the Group assessments pop-up.
   For more information on the response types, see Consolidate control attestations using the Same Response feature.
6. Select a criterion to group the assessments in the **Group by** list.
   By default, assessments are grouped by the metric type template. You can group the assessments by Category, Entity, or Control objective. If the selected assessments have a common category, entity, or control objective then they're grouped accordingly based on your selection. However, if the assessments selected don't have any of the common criteria by which they can be grouped, then the assessments aren't grouped.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **Group previews** section displays the grouping details, assessments with links, and an appropriate message information if they're grouped or cannot be grouped based on the Group by criterion, status, assignee, or the evaluation method of the metric type.

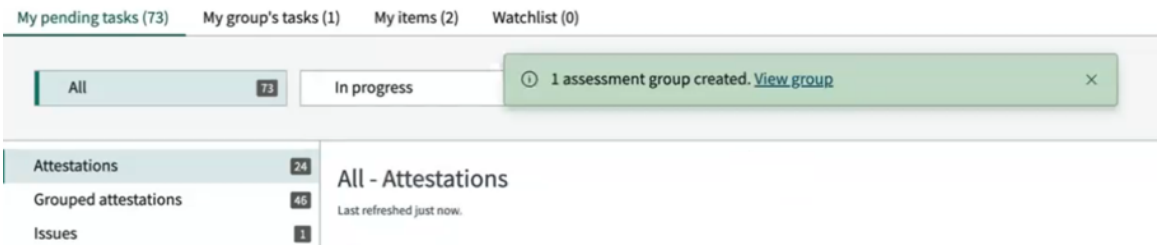



7. Select the **Group** button.
   If the grouping of assessments is successful, then you get a message indicating that the assessment group has been created, followed by a link to the grouped assessments.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

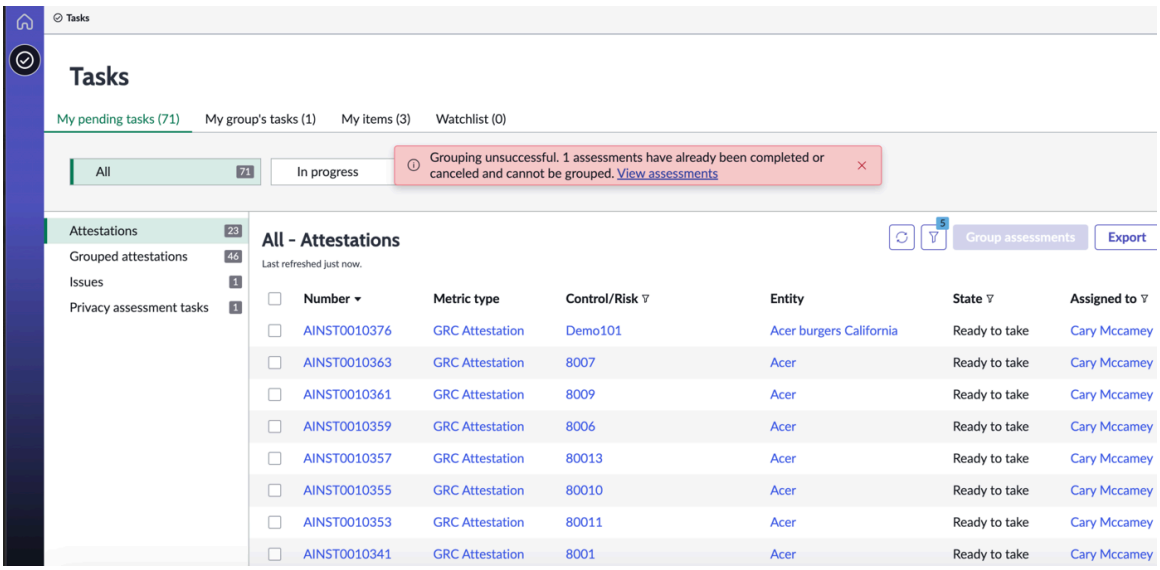
If a few of the assessments among the selected assessments couldn't be grouped by the selected criterion, then the **Group previews** displays the number of assessments that couldn't be grouped. Nevertheless, as there are other assessments in your selection that could be grouped by the selected **Group by** criterion, the **Group** button is active for you to select and group the rest, where the grouping is successful.

On the other hand, if all the assessments that you selected are invalid, for example, risk assessments or privacy assessments, then the **Group** button is inactive as grouping isn't possible for such assessments.




**Note:** You can group the assessments that are in **Ready to take** or **In progress** state, but not the assessments that are in **Complete** or **Canceled** state.

If the status of a record that you've selected for grouping has changed and is being assessed before you select the **Group** button to group the assessments, then such a record can't be grouped.




8. Select the link to the grouped assessment in the UI message.
   The link takes you to the list view of the grouped assessments. The Assessment Instance page opens up, where you can take the assessment.

### Manage control indicators using the Compliance Workspace

Continuous monitoring involves activities related to identifying and creating key risk and controls indicators. The Compliance Overview is available to compliance administrators and compliance managers, providing an executive view into compliance requirements, overall compliance, and compliance breakdowns.

Supporting information can be collected for indicators through automatic data collection or manual tasks. Indicator results are then used to create issues for controls, update risk scores, and provide supporting information for audit activities and control testing.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Indicators

Indicators collect data to monitor controls and risks, and collect audit evidence. Indicators monitor a single control or risk.

Indicator templates

Indicator templates allow the creation of multiple indicators for similar controls or risks.

## Compliance Overview

### Compliance Overview reports in the base system

| Name | Visual | Description |
|---|---|---|
| Compliance Requirements | Donut chart | Select a wedge to focus on a specific compliance area. |
| Overall Compliance | Donut chart | Displays the overall compliance of all the control requirements in the system. Selecting a specific wedge in the previous widget brings that area into focus. |
| Entity | Drop down list | Select one or more entities to view and compare their compliance across multiple items. |
| Control State | Check list | Select or clear check boxes to view filter reports by control state. |
| Compliance by Authority Document | Bar Chart | Compare level of compliance depending on the selected entity and/or authority document. |
| Compliance breakdown | Multi-level Pivot | View a breakdown of control compliance by related authority documents and policies. |
| Non Compliant Entities | Column Chart | Count of non-compliant control requirements grouped by entity. |

## Authority Documents

Authority documents define policies, risks, controls, audits, and other processes to ensure adherence to the authoritative content.

Each authority document is defined in a record and the related lists on that record contain the individual conditions of the authority document.

The relationships of these authority document related list items are visible in the GRC Workbench in the Policy and Compliance Management application.

**Note:** You can add content reference tags to authority documents. Content reference tags allow you to filter records in order to more easily identify the content packs, integrations, and use case accelerators associated with the authority documents.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Citations

Citations contain the provisions of the authority document, which can be interrelated. Citations break down an authority document into manageable themes.

You can create citations or import them from UCF authority documents and then create any necessary relationships between the citations.

**Note:** You can add content reference tags to citations. Content reference tags allow you to filter records in order to more easily identify the content packs, integrations, and use case accelerators associated with the citations.

### Create a control indicator using the Compliance Workspace

Indicator data for controls, risk, and audit evidence are measured differently depending on the GRC application.

#### Before you begin

Role required: sn_compliance_admin, sn_compliance_manager

#### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Control monitoring** > **All indicators**.
   - **Risk** > **Control monitoring** > **All indicators**.
   - **Audit** > **Control monitoring** > **All indicators**.
2. Click **New**.
3. On the form, fill in the fields.

**Indicator form**

| Field | Description |
|---|---|
| Category | The type of indicator being created. Select **Compliance Indicator** for a control indicator and **Risk Indicator** for a risk indicator. |
| Inherit from template | Use a selected template to fill in the form. |
| Template | If you selected the **Inherit from template** check box, select the template you want to use to fill in the form. After you have selected a template, the rest of the fields in the Create New Indicator screen are pre-filled and set to Read-only. For more information, see Create a GRC indicator template using the Compliance Workspace. |
| Override template | If you selected the **Inherit from template** check box, and you want to customize your entries in the form, select this check box. You can then edit some or all of the fields on the form. |
| Name | Name of the indicator. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Description | A description of this indicator. |
| Entity | Entity associated with this indicator. |
| Control | Control associated with this indicator. |
| Owning group | Group that owns the indicator. |
| Owner | Indicator owner. |
| Method | |
| Type | Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script.<br>◦ Manual<br>◦ Basic<br>◦ Script |
| Applies to | Entity related to the **Item**. |
| Last result passed | Option that indicates whether last result passed. |
| Short Description | If Type is **Manual**, this field is present. Brief description of the issue. |
| Instructions | If Type is **Manual**, this field is present. Instructions for the collection of indicator results. |
| Value Mandatory | If Type is **Manual**, this field is present. |
| Passed/Failed | If Type is **Basic**, this field is present. Indicator passes or fails. |
| PA Threshold | If Type is **PA Indicator**, this field is present. The associated PA Threshold. |
| Script | If Type is **Script**, this field is present. Script that obtains the desired system information. |
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| Next run time | Next collection time for indicator results. |
| Supporting Data | |
| **Note:** Starting with Version 10.1, the actual historical data for the supporting data records from the indicator results or indicator tasks is displayed. Earlier, only the real-time state of the records collected could be viewed. | |
| Table | Use supporting data to gather supporting evidence from other applications. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Supporting data fields | Supporting data fields based on the selected table. |

4. Click **Submit**.

### What to do next

If you are implementing the Policy and Compliance Management software, you have completed the mandatory setup steps. Return to the Policy and Compliance Management setup checklist and proceed to the optional steps, as needed.

## Create a GRC indicator template using the Compliance Workspace

Compliance or risk managers create indicator templates in the Compliance Workspace from which many indicators can be created.

### Before you begin

Role required:

- sn_compliance.admin or sn_compliance.manager
- sn_risk.admin or sn_risk.manager
- sn_audit.admin or sn_audit.manager
- sn_grc.user

### Procedure

1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Compliance Workspace** > **Indicators** > **Indicator Templates**.
   - **Risk** > **Indicators** > **Indicator Templates**.
   - **Audit** > **Indicators** > **Indicator Templates**.
2. Select the **Create** list and click **Indicator**.
3. Select **New**.
4. On the form, fill in the fields.

#### Indicator template form

| Field | Description |
| --- | --- |
| Name | Name of the indicator. |
| Description | Description of the indicator. |
| Category | Category for which you're creating an indicator template. For example, select **Risk Indicator Template** to create a risk indicator template. |
| Active | Option that determines whether the indicator template is active. |
| Method | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Type | Method used to determine the type of indicator template. The choices are as follows:<br>◦ **Manual**: Manual indicators are used for data that can't be retrieved from a ServiceNow instance because it comes from an external system, such as customer data from a third-party sales system.<br>◦ **Basic**: Basic indicators are automated indicators based on an indicator source. The indicator source specifies a table and a frequency at which the scores from this table are saved.<br>◦ **Script**: Scripted indicators use a custom script to collect the data. |
| Target Type | Type of the target value. The choices are as follows:<br>◦ **None**: Use this option if you don't want to set up any target or threshold for the indicator.<br>◦ **Percentage**: Use this option to determine the indicator result by a percentage value.<br>◦ **Count**: Use this option to determine the indicator result by a count value or total number. |
| Result if the value meets or exceeds the target value | Result configuration field. The choices are as follows:<br>◦ **Passed**<br>◦ **Failed**<br>For example, assume you enter `100` in this field. If the indicator result output is more than 100, then the indicator status will pass or fail based on the value configured in this field. |
| Target | Value to determine if the indicator will pass or fail. |
| Value mandatory | Option to decide if a value must be compulsory in the indicator task for a manual indicator.<br>**Note:** This option appears only if **Manual** is selected from the **Type** field. This option is automatically selected if **Count** or the **Percentage** is selected from the **Target type** field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Instructions | Additional instructions for the template. |
| Supporting Data | |
| **Note:** Starting with version 10.1, the actual historical data for the supporting data records from the indicator results or indicator tasks are displayed. Earlier, only the real-time state of the records collected could be viewed. | |
| Collect supporting data | Option to enable collecting supporting data or evidence every time the indicator runs. |
| Table | Table used for collecting supporting data. |
| Supporting data fields | Fields of the source table to be used for collecting the supporting data. |
| Sample size | Minimum number of records that must be used for collecting supporting data.<br><br>For example, a basic indicator could query a large table, returning thousands of records with each indicator execution. You don't have to save all of them; just a sample of those records. If you enter a sample size of 100, only 100 records are saved, even though the query returned thousands. |
| Basic Criteria | |
| Criteria | Criteria to filter the data from the source table. |
| Use reference field | Option to enable the use of the **Reference field**. |
| Reference field | Connection between the supporting data table and the **Applies to record** field of the entity. |
| Additional Criteria | |
| To create indicators with targets, use the advanced filter criteria. This section appears only when you select **Basic** from the **Type** field. This section is used to provide more filter criteria. | |
| Additional criteria | More criteria to filter the data to calculate the target value. This section only appears when **Percentage** is selected from the **Target type** field. |
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Due date duration (days) | Due date duration in days between the creation and due date of the indicator task and generation of its results.<br><br>The due date duration added to the creation date reflects as the **Due date** of the indicator task.<br><br>This field appears only when **Manual** is selected from the **Type** field.<br><br>For more information, see Performance enhancements for Indicator nightly job. |
| First run date | First collection time for indicator results. This field is automatically set based on when an indicator or an indicator template runs for the first time. This value in this field cannot be modified. |
| Next run date | Next run time to collect indicator results of all downstream indicators for this indicator template. |

5. When you have completed these entries, you can also view information on the following related lists:
   - Control Objectives/Risk Statements
   - Content References

   **Note:** The **Control Objectives/Risk Statements** tab enables you to reuse the same template for multiple control objectives or risk statements, or both of them.

6. Select **Submit**.

### Performance enhancements for Indicator nightly job

To support parallel processing capabilities, two additional custom queues such as the Indicator Data Queue for processing indicators, and the Supporting Data Queue for handling events related to control, risk, and issue updates, and to collect the supporting data have been introduced.

## New architecture for effective processing of indicators

The execution of indicators has been optimized by implementing a three-step process, utilizing two custom queues for efficient processing.

In the initial step, a set of indicators requiring processing is queued up in the Batch Indicator Data Queue. The Batch Indicator Data Processor then runs the indicators, sets the status, and creates the indicator results or tasks. The indicators are then moved to another custom queue for supporting data collection and updating dependent objects like controls, risks, and issues.

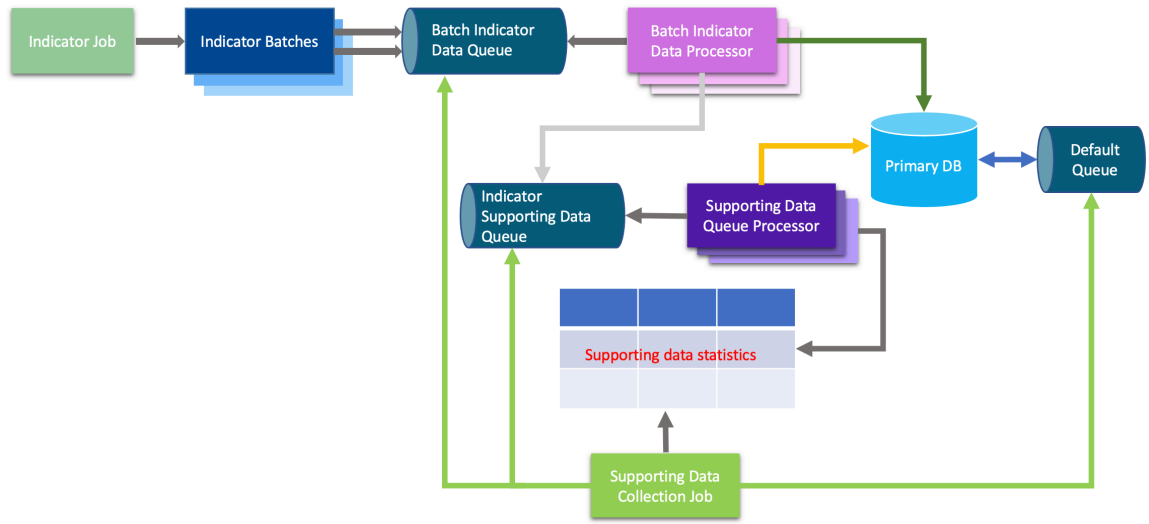
In the second step, the Indicator Supporting Data Processor picks up the indicator records from the Indicator Supporting Data Queue and updates the control or risk status, also creating or updating issues based on the configuration. Then the indicator is pushed to the Indicator Statistics Table for support data collection.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Finally, the Supporting Data Collection Job picks up the indicator records from the Supporting Data Statistics Table, starts collecting supporting data for the indicators, and leverages both the default queue and additional custom queues for efficient processing.

**Note:** Indicator result business rules are not executed during the indicator job run. However, the same business rules are used while completing the indicator task. The indicator business rules are moved to the indicator job for achieving better performance during the execution.

**Processing indicator jobs using additional queues**




This architecture supports execution of a large number of indicators in significant time. The Supporting Data Collection Job introduced to collect supporting data improves the data handling process considerably. Moreover, the time taken to execute the data is considerably less.

**Note:** The Supporting Data Collection Job assigns the batches of indicator records to the default queue initially for supporting data collection. Depending on the availability of the batch processing queue and supporting data queue, the scheduled job assigns the subsequent batches of indicator records to these queues in a round-robin fashion, that is, only if these queues are free to process them.

## Data model changes

The **Sample collection type** field added in the Indicator template form, has options either **Count** or **Percentage**. The default value is Count. If you select Percentage, you can provide the percentage value to collect the supporting data.

The **Due date duration (days)** field is added for manual indicator in the Indicator template and Indicator forms to capture the indicator task due date. Based on this due date, reminder emails are sent to the indicator task owners.

A new field introduced in the indicator supporting data table, which is of type JSON, helps in efficient data management.

- For more information related to the table changes, see .
- For more information on the additional system properties, see .
- For Indicator form changes, see Create a GRC indicator.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- For the Indicator template form changes in Compliance Workspace, see Create a GRC indicator template using the Compliance Workspace.
- For the Indicator template form changes in the classic UI, see Create a GRC indicator template.

### Manage evidence requests using the Compliance Workspace

Evidence request is used by audit and compliance teams for requesting supporting documents during an audit. Auditors and compliance teams require these documents from the first line of defense.

Evidence request: Evidence is all the information used by an auditor in determining the audit opinion. Evidence includes the information contained in the accounting records underlying the financial statements and other information. Evidence is cumulative in nature. It includes evidence obtained from audit procedures performed during the audit. Evidence may also include audit evidence obtained from other sources such as, previous audits.

An evidence request is frequently introduced during the audit preparation or planning phase after the audit announcement. The documents requested are used by the audit team to understand the in-scope controls and processes, and to begin fieldwork testing. As an audit progresses through various stages, the audit team frequently adds new requests to the list. The compliance teams use the collected evidence for control testing.

Starting with version 11.0.2 release, an unplanned evidence request is supported by the Audit Management and Policy and Compliance Management applications in the following ways.

- Evidence can be requested from an engagement and all audit tables. To understand how to request evidence, see Request evidence for audit.
- Compliance teams can request evidence from control owners, business stakeholders, and process owners.
- Audit teams can request evidence from control owners, business stakeholders, process owners, and compliance teams.
- Assigned users can provide evidence directly from the Service Portal.
- Managers can approve evidence requests based on various criteria, such as confidentiality and criticality.
- Improved communication channels between requesters and assignees streamline the approval process.
- Improved confidentiality constraints prevent unauthorized persons from viewing request information.

### Request evidence during audits using the Compliance Workspace

Request evidence at any stage during an audit using the Compliance Workspace. The details about the items for which evidence is requested are also provided to the person responsible for providing the evidence.

#### Before you begin

Role required: sn_audit.user

#### About this task

Evidence can be requested in the following three ways:

My Evidence

By creating an evidence record from the **My Evidence** module.

Request Evidence

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

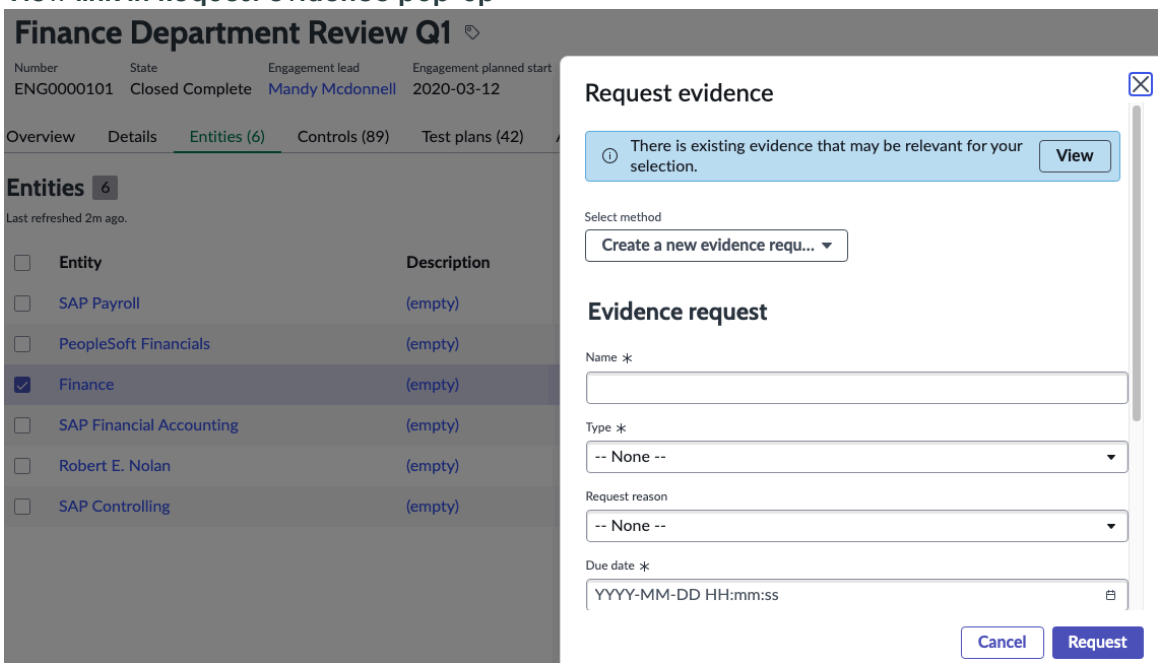
From the Entity, Control, Audit Task, Control Test Issue, and Other Issues related lists in an engagement record. To request evidence from these sources, navigate to **All** > **Policy and Compliance** > **Compliance Workspace**. In the List view of the workspace, select **Engagements** in the Control testing list. Open the engagement record, and select the related list from which you want to request evidence. Select the **Request Evidence** button. Here, you can either create an evidence request or add more requests to an existing evidence request. The Evidence request is created but not the evidence request tasks.

You can inform the user of the evidence records that already exist for any of the related item tables of the engagement, which they can reuse.

1. To create a new evidence request, select **Create a new evidence request** in the **Select method** list of the Request Evidence pop-up. Enter the details and select the **Request** button.
2. To view the information about existing related evidences, select the **View** link in the Request Evidence pop-up.

   **Note:** If there is no existing evidence, then the message does not appear in the Request Evidence pop-up.

   **View link in Request evidence pop-up**




3. To view all existing evidences created on the related items, select the Evidence related list.

   When the evidence is in **Closed Complete** state, the UI action buttons such as **New**, **Add existing evidence**, **Remove**, and **Delete** are disabled. You can perform these UI actions only when the engagement or any other audit and compliance object is in an active state.

4. To add existing evidence, select the **Add Existing Evidence** button and select the evidence.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** The **Add Existing Evidence** button is available in the Evidence related item of all compliance and audit objects in the Compliance Workspace such as Engagement, Audit task, Issue, Policy, Entity, Control, Control Objective, Authority document, Citations, and Evidence request.

5. To remove the association of the evidences linked to the engagement, select the evidences in the Evidence related list and select the **Remove** button.

**Note:** The action only removes the association of the existing evidence records from the engagement and doesn't remove the evidence record from the database.

**Note:** The logged-in user must also have access to the engagement for which evidence records exist or must be the user who has access to the record to view and add them. If the logged-in user doesn't have access to those records, although there are evidenced existing on those related items, they aren't displayed for the user to add.

Entity, Control, Control Objective, Control Test, Engagement, Issue tables

From tables such as Entity, Control, Control Objective, Control Test, Engagement, Issue. However, when the users request evidence from these tables, the evidence request is created not the actual evidence request task. The users must navigate to the evidence request record that is generated and then add evidence request tasks.

In this procedure, the method to request evidence from the **My Evidence** module is described.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the List icon ( ).
3. Navigate to **Evidence requests** > **My request**.
4. Select **New**.
5. On the form, fill in the fields.

**Evidence Request form**

| Field | Description |
|---|---|
| Number | Unique number of the evidence request. |
| Name | A name for this request. |
| Requester | User requesting evidence. This field is automatically populated. |
| Requested on behalf of | User for whom evidence is being requested. |
| Type | Type of evidence that is created. Can be either Audit or Compliance. |
| Request reason | Reason for requesting evidence. |
| State | State of the request. The default state is **Draft**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Substate | An additional state for the request. |
| Description | Detailed description of the evidence request. |
| Assignment | |
| Assignment group | Group assigned to provide evidence. |
| Assigned to | User responsible for providing the evidence. |
| Watch list | Users interested in viewing the evidence collected. If a person is added on the watch list, they can navigate to **Audit** > **Evidence Request** > **Watched Evidence Requests** to view the requests. |
| Schedule | |
| Due date | Expected date of evidence submission. |
| Opened | Date the request is opened. This date is automatically updated. |
| Closed | Date the request is closed. This date is automatically updated. |
| Activity | |
| Work notes | Type any notes that might be required. |
| Activities | Activity log for the request. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on the confidential option, see Confidentiality flag for audit and compliance records. |

6. Save the form.
   Monitor the state of the Evidence in the stepper of the Overview page. The record progresses through a sequence of logical steps when you accept evidence, request revision of the evidence, and request information.

   The Evidence collection details related list appears. This related list is used to list the items for which evidence is requested.

7. Select **New**.
8. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Evidence collection details form

| Field | Description |
|---|---|
| Number | Unique number for the evidence collection detail. |
| Name | A name for this request. |
| Evidence collection type | Record for which evidence is requested.<br><br>If the request was entered by a user with the compliance user role, the available options are:<br>◦ Authority document<br>◦ Citation<br>◦ Control<br>◦ Control objective<br>◦ Control test<br>◦ Entity<br>◦ Issue<br>◦ Policy<br><br>If the request was entered by a user with the audit user role, the available options are:<br>◦ Audit task<br>◦ Control<br>◦ Control objective<br>◦ Control test<br>◦ Engagement<br>◦ Entity<br>◦ Issues |
| Evidence for | Lists all the tables to which the evidence is applied. |
| Evidence request | Unique number of the evidence request task. |
| Assignment | |
| Assignment group | Group assigned to provide evidence. The users of this group must have the sn_grc.business_user roles. |
| Assigned to | User responsible for providing evidence. |
| Instructions | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Evidence collection instructions | Instructions for providing evidence. For example, list of supporting documents, files, and so on. |

9. Select **Save**.
10. Select **Request Evidence**.
    When an evidence request is already in the Work in Progress state, and a new evidence collection detail is added, the evidence request task is sent to the assignee immediately. The Evidence related list appears with the list of evidences and the person who is assigned the request receives an email notification to provide the requested evidence. Also, the state of the request changes to **Work in Progress**.You can view the description and monitor the state of the Evidence request in the stepper of the Overview page as it progresses through the evidence request process flow.

### Provide requested evidence using the Compliance Workspace

Using the Compliance Workspace, you can provide evidence when you are requested. When evidence is requested, the person who must provide the evidence receives an email. The process to provide the evidence begins.

#### Before you begin
Role required: sn_grc.business_user, sn_grc.business_user_lite

#### About this task
When the assignee receives the email to provide the requested evidence, the assignee can either provide the requested evidence or reassign the request to another user. The assignee can also add approvers before sending the requested evidence to ensure additional security of the evidence. If the assignee reassigns the request to some other user, the original assignee can no longer view the request. If the evidence provided does not need an approver, then the assignee can directly request a review of the evidence, and the requester gets a notification to review the evidence.

#### Procedure
1. Navigate to **Audit** > **Evidence Request** > **My Evidence Request Tasks**.
2. Open the record for which you want to provide evidence.
3. Click **Accept Work**.
4. On the form, fill in the fields.

**Evidence form**

| Field | Description |
|---|---|
| Number | Number of the evidence request. This value is generated by default. |
| Requester | User requesting evidence. This value is generated by default.<br><br>If you are the approver, requester, watch list member, or user in the Assigned to field, then you can edit the details in the **Watch list**, **Name**, and **Description** fields when |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | the evidence is in **New** or **Work in progress** states. |
| Requested on behalf of | User for whom evidence is being requested. This value is generated by default. |
| Assignment group | Group assigned to provide evidence. The users of this group must have the sn_grc.business_user roles. |
| Assigned to | User responsible for providing the evidence. This value is generated by default. |
| State | State of the request. |
| Substate | None. This value is generated by default. |
| Request reason | Reason for requesting evidence. |
| Approvers | Users to approve evidence before it is returned to the requester for review. Usually, an approver is the manager of the person providing the evidence. |
| Watch list | Users interested in viewing the evidence collected. |
| Name | Name of the evidence request. The name defaults to Evidence collection details name. |
| Description | Detailed description of the evidence request. The description defaults to the description given in the Evidence request form. |
| Request Details | |
| Evidence request | Unique ID of the evidence request associated with the task. This value is generated by default and is fetched from the record that was created to request evidence. |
| Evidence for | Record for which the evidence is requested. |
| Evidence for description | Description of the record for which the evidence is being requested. This value is generated by default and is fetched from the record that was created to request evidence. |
| Evidence collection instructions | Instructions to collect the evidence.<br><br>If you are the manager or requester, you can edit this field when the evidence request task is in work in progress state. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. To request approval for the attached evidence, click **Request Approval**.
6. If no approvers are required, click **Request Review**.

### Approve evidence before evidence review using the Compliance Workspace

Using the Compliance Workspace, approve the evidence being provided before the requester views the evidence. When evidence is provided in response to an evidence request, the evidence may need an approval before the evidence is sent back to the requester. This ability ensures security and confidentiality of the evidence.

#### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

#### About this task

After receiving a request to approve evidence, an approver can do one of the following:

- Approve the request if there are no issues or concerns.
- Request revision of the evidence attached in case it is not correct or needs rectification.
- Request information if the approver wants more details about the attached evidence.

#### Procedure

1. Navigate to **Audit** > **Evidence Request** > **My Approvals**.
2. Open the record for which you want to approve evidence.
3. Review the attached evidence on the form and click one of the following options:

| Option | Description |
|---|---|
| **Approve** | Approve the attached evidence. The requester gets the evidence provided. |
| **Request Revision** | Request that the attached evidence be reviewed. Enter comments when you request revision. The assignee gets a notification to review the attached evidence. |
| **Request Information** | Seek more information and details about the attached evidence. The assignee gets a notification to provide more information about the attached evidence. |

### Accept, reject, or cancel an evidence request using the Compliance Workspace

Accept, reject, or cancel an evidence request when you receive the evidence you requested. After requesting an evidence request using the Compliance Workspace, when the requester receives the evidence, the requester can accept, reject, or cancel the evidence request.

#### Before you begin

Role required: sn_compliance.user

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **Audit** > **Evidence Request** > **My Pending Reviews**.
2. On the Evidence form, review the attached evidence, and click one of the following options:

| Option | Description |
|---|---|
| **Accept Evidence** | Accept the evidence that is provided. |
| **Request Revision** | Request for the evidence to be reviewed, if it is not appropriate, or modified. |
| **Cancel** | Cancel the evidence request task. |
| **Delete** | Delete the evidence request task. |

#### Review related evidence using the Compliance Workspace

The Evidence Request feature includes a related list called Related Evidence that is not visible by default.

### Before you begin

Role required: admin

### About this task

This related list provides a list of evidence that is not directly requested for the current record, but is associated to a related record. For example, the Related Evidence list on the Control Objective form shows evidence requested for associated controls.
The Related Evidence related list is available to a wide variety of forms throughout the Evidence Request feature; however, it is not visible in the base system. You can personalize any of the forms in which it is available, but keep in mind that activating this related list can impact system performance.

#### Tables that can display the Related Evidence related list

| Table name | Type of related evidence displayed |
|---|---|
| Authority document | Evidence request tasks created on the citations mapped to this authority document. |
| Citation | Evidence request tasks created on the control objective associated to the citation. |
| Control | Evidence request tasks created on the control test mapped to the control and Issues created for the control. |
| Control objective | Evidence request tasks created on the controls associated to the control objective. |
| Control test | Evidence request tasks created on the controls associated to the control test. |
| Engagement | Evidence request tasks created on the entities, controls, control tests, audit tasks, control test issues, and issues mapped to the engagement are displayed. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tables that can display the Related Evidence related list (continued)**

| Table name | Type of related evidence displayed |
|---|---|
| Entity | Evidence request tasks created on the controls associated to the entity, Issues created on the entity. |
| Policy | Evidence request tasks created on the control objective associated to the policy. |

### Procedure

1. Navigate to the form for which you want to display the **Evidence Request** related list.
2. Right-click in the form header, and click **Configure** > **Related Lists**.
3. Locate the **Related Evidence** item in the **Available** box and move it to the **Selected** box.
4. Click **Save**.

## Policy authoring and redlining in Compliance Workspace

Policies are effective when they're carefully monitored and revised periodically. By reviewing and updating them at regular intervals, organizations can maintain updated policies to avoid audit and compliance risks.

Policies of an organization tend to get outdated over time either due to the growth of the organization or due to the changes that happen in an organization structure. For these reasons, policies must be carefully monitored and revised consistently.

Policy owners, collaborators, reviewers, and approvers enable policy authoring and redlining. Review and redlining of policy results in multiple versions that must be maintained for an audit purpose.

Key benefits of policy redlining

It improves the overall policy authoring and redlining experience by enabling:

- Policy owners, collaborators, reviewers, and approvers to collaborate using O365 or Google Drive.
- Redlining and reviewing capability.

Key features

1. Policy owners and collaborators can collaborate and draft a policy using O365 or Google Drive.
2. Policy reviewers can collaborate, review, and redline policy.
3. Approvers can review and approve the policy.
4. Ability to maintain different versions of the policy, and retain its history.
5. Ability to copy policy text from a document to the policy text field in HTML, retaining the format.
6. Ability to convert the policy to PDF format.
7. Simplify user experience by guiding the user through policy authoring, redlining, and publishing.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Import policy text for redlining

Import the policy text as an attachment if you're unable to do the word editing.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst; mp_document_user

### About this task

You can import the content only when you're the policy owner and the policy must also be in Draft state.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the List icon (  ).
3. Navigate to **Compliance library** > **My policies**.
   You can create a new policy or open a record to enable the redlining feature.
4. Select a policy to open.
5. Select a Policy text related list to view the contents of the policy text.
   If you do not have Microsoft OneDrive or Google Drive integration, then you can import the policy text as an attachment. You can import the content only when you're the policy owner and the policy must also be in Draft state.
6. Navigate to **All** > **Policy and Compliance** > **Administration** > **GRC properties**.
7. Select the option **None** in the *Select a file sharing service to host documents and attachments* system property list.

   a. Select the **Import policy text** button.

   b. Select **Add File** in the Import policy text pop-up.

   c. Select **Import**.
   The content of the file is downloaded in the **Policy text** field.

## Pre-requisites to enable policy redlining feature

Certain configurations are required to be set up for policy collaborators to use the policy redlining feature in the Compliance Workspace.

For Policy authoring – integration with O365, you require these spokes

- Microsoft OneDrive Spoke version 2.1.1
- Microsoft OneDrive Spoke for Document Service Framework version 1.0.5

For Policy authoring – integration with Google Drive, you require these spokes

- Document Service Framework for Google Drive Spoke – 1.0.1
- Google Drive Spoke – 1.4.1

**Note:** Integration Hub entitlements included in the Compliance Workspace are for Policy authoring – integration with O365. Using Microsoft OneDrive integration requires Integration Hub transactions not included in the Compliance Workspace product but requires an Automation Engine or Integration Hub subscription.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you're a policy collaborator wanting to use the policy redlining feature in the Compliance Workspace, then you must set up the following configurations.

**Note:** You can establish a connection with only one of the following cloud hosting services: either Microsoft OneDrive or Google Drive

Establish a connection with cloud hosting services

Connection with Microsoft OneDrive

1. You must first set up the Microsoft OneDrive and Microsoft Azure AD connections to perform actions in Microsoft OneDrive from ServiceNow. For more information, see Setup Microsoft OneDrive for Document Services.
2. Then, execute the sync collaborators schedule job. To execute the job, see Microsoft OneDrive Spoke for Document Services Framework.

Connection with Google Drive

To set up Google Drive as a cloud hosting service and to create or update the policy text document that resides in Google Drive, you must:

1. Set up account.
2. Integrate the Document Services with Google Drive. For more information, see Document Services framework for Google Drive Spoke.

Enable system properties to use policy redlining in Compliance Workspace

1. Navigate to **Policy and Compliance** > **Administration** > **GRC properties**.
   a. To opt Microsoft OneDrive as your cloud hosting service, select **One drive** in the *Select a file sharing service to host documents and attachments* system property list.

      If you select **None** in the *Select a file sharing service to host documents and attachments* system property list, then you can import the policy text. For more information, see Import policy text for redlining.

   b. To opt Google Drive as your cloud hosting service, select **Google drive** in the *Select a file sharing service to host documents and attachments* system property list.
2. Set the folder path that is to be created in Microsoft OneDrive in the *Default folder path where documents and attachments will be located. You can organize files in sub-folders within this path* system property list.

Provide mp_document_user role

The mp_document_user role is required to access policy redlining document-related tables. This role is required for users using the policy redlining feature to create, update, and delete the related documents.

As a sys admin you can establish the cloud hosting connection, enable system properties, and provide the mp_document_user role for the policy redlining users.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Create and associate a policy text document for policy redlining

Create and enable the policy with the redlining feature. When you create such a policy, another record is created in an internal table that records the version history of the policy.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst; mp_document_user

### About this task

**Note:** Policy redlining is enabled only for policy authoring in Compliance Workspace and not in Now Platform.

Although policy redlining as a feature is not available in Now Platform, the following changes that are made in Compliance Workspace to enable redlining for a policy are also visible in the policy form if you access it in Now Platform:

- Owner field is required.
- Approvers must be identified before you request approval. Previously, the policy can be auto-published even if there was no approver.
- Contributors field is added.
- Policy history related list is available.
- Activity field is added.

However, these changes support the redlining feature of the policy in Compliance Workspace and do not support any policy-related activities on Now Platform.

Contextually, Cloud refers to documents that reside in both Microsoft OneDrive and Google Drive.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the List icon ( ).
3. Navigate to **Compliance library** > **My policies**.
   You can create a new policy or open a record to enable the redlining feature.
4. Select a policy to open.
5. For Microsoft OneDrive, select the Policy text related list to view the contents of the policy text.

   a. Select the **Enable document editing** button.
   If the policy is in **Draft** state, then the policy owner can alone create a document or associate a document from Microsoft OneDrive to enable the policy text for editing by the approvers, reviewers, and contributors.

   b. To create a document as a policy owner, select **Create new document** in the **Enable document editing** list.

   c. Enter the path of the folder where the document resides in the **Folder location** field.

   d. Enter the name of the document in the **Document name** field.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

e. Select **Create**.

f. To view the document that is created, select the **Open in Word** button.

6. For Google Drive, select a Policy text related list to view the contents of the policy text.

   a. Select the **Enable document editing** button.
   If the policy is in **Draft** state, then the policy owner can alone create a document or associate a document from Google Drive to enable the policy text for editing by the approvers, reviewers, and contributors.

   b. To create a document as a policy owner, select **Create new document** in the **Enable document editing** list.

   c. Copy the shareable folder link from Google Drive and paste it in the **Folder link** field in the Create a document pop-up.

   d. Enter the name of the document in the **Document name** field.

   e. Select **Create**.
   On selecting create, the document is created in the folder of the Google Drive account that you provided. If you're providing a link to a shared folder, then you must have edit access to create a file within that folder.

   f. To view the document that is created, select the **Open in Google docs** button.

7. To view the users that have read or write access to the document, navigate to the Document access related list.
8. To create another document or connect to a different document for a redlining-enabled policy, select the **Change document** button.
   - To create another document, select **Create new document** that opens the Create a document pop-up.
   - To connect to a different document, select **Connect existing document** that opens a Connect existing document pop-up.
9. To update the content of the document in the **Policy text** field, select the Update link below the document link.
10. If the policy has been drafted and complete, the policy owner can request a review by selecting the **Request review** button.
11. Enter a message for the reviewers in the Request review pop-up.
12. Select **Request**.
    As a reviewer, you can view the policy, if ready for review, when you log in to **My pending tasks** in the Tasks view.
13. Select the **Submit review** button.
    You can review the policy text, add a comment in the Submit review pop-up, and submit it.
14. To preview the document and to get the latest update after your collaborators have edited, select the Update link in the **Policy text** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

As a policy owner, you can edit the content of the document in either Microsoft OneDrive or Google Drive to maintain a sync between the document in Cloud and the policy text field of the policy.

All activities between the policy owner and the reviewers are captured in the **Activity** tab of the **Details** related list. If all reviewers have completed the review, then the policy owner can complete the publishing checklist.

15. Select the **Complete publishing checklist** button.
    If all reviews are complete, then as a policy owner you can complete the publishing process. This action creates a playbook. The policy owner must go through the publishing checklist before requesting approval. See, Complete publishing checklist for the policy and request approval.
16. To view the history of the policy, select the Policy history related list.
    For more information, see View the history of a redlining-enabled policy.

## Connect an existing document from Microsoft OneDrive to policy

Enable redlining in a policy document that is existing in your Microsoft OneDrive instead of creating a document in Microsoft OneDrive.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst; mp_document_user

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the List icon ( ).
3. Navigate to **Compliance library** > **My policies**.
4. Select a policy.
5. Select a Policy text related list to view the contents of the policy.
   If you already have a document on Microsoft OneDrive with some content in it, which you want to associate with the policy, then you can associate that document.
6. Select the **Enable document editing** list.
   If the policy is in **Draft** state, then only the policy owner can associate a document from Microsoft OneDrive to enable the policy text for the approvers, reviewers, and contributors to edit.
7. To link an existing document with the policy that is enabled for redlining, select **Connect Existing document** in the Enable document editing list.
   a. Enter the location of the folder in the **Folder location** field.
   b. Enter the name of the document in the **Document name** field.
   c. Select **Connect**.
   d. To open the document, select the link.
   e. To update the content of the document in the **Policy text** field, select the Update link below the document link.
   You can still create another document or connect to a different document for a policy that is already enabled with redlining.
8. To create another document or connect to a different document for a redlining-enabled policy, select the **Change document** button.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- To create another document, select **Create new document** that opens the Create a document pop-up.
- To connect to a different document, select **Connect existing document** that opens a Connect existing document pop-up.

**a.** Enter the path of the folder where the document resides in the **Folder location** field.

**b.** Enter the name of the document in the **Document name** field.

**c.** Select **Create**.

**d.** To update the content of the document in the **Policy text** field, select the Update link below the document link.

## Connect an existing document from Google Drive to policy

Connect a document that exists in your Google Drive folder to a policy that you created. Use this existing document and enable redlining in the policy text instead of creating a document.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst; mp_document_user

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the List icon ( ).
3. Navigate to **Compliance library** > **My policies**.
4. Select a policy.
5. Select a Policy text related list to view the contents of the policy.
   If you already have a document on Google Drive with content in it, which you want to associate with the policy, then you can associate that document.
6. To connect a document that is in your Google Drive folder.
   a. Navigate to My Drive in https://drive.google.com/
   b. Select the document that you want to connect to the policy.
   c. Select the More actions icon ( ⋮ ) in the document that you want to connect.
   d. Select the **Copy link** option from the **Share** list.
7. Navigate back to the Policy text related list of the policy record.
8. Select the **Enable document editing** list.
   The policy must be in **Draft** state, only then the policy owner can associate a document from Google Drive to enable the policy text for the approvers, reviewers, and contributors to edit.
9. Paste the copied Google Drive in the **File link** field of the Connect existing document pop-up.
10. Select **Connect**.
    You should be able to connect the document from the Google Drive to the policy record.
11. Select Update.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Policy text field displays the text from the Google Drive document in the ServiceNow policy record.

**Note:** For more information on Google Drive Integration for Policy authoring and redlining, see the Google Drive Integration for Policy authoring and redlining – General guidelines and Known limitations [KB1587198] article in the Now Support Knowledge Base.

## Sync document and view policy text

Update the document and view the content in the Policy text field.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst; mp_document_user

### About this task

Contextually, Cloud refers to documents that reside in both Microsoft OneDrive and Google Drive.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the List icon ( ).
3. Navigate to **Compliance library** > **My policies**.
4. Select a policy to open.
5. Select the **Policy text** tab to view the contents of the policy.
6. Select **Update**.
   The **Policy text** field is updated with the latest content from the document.

   As there are many collaborators on the policy, you must update the content to get the latest update. Last sync information helps you to know when the document was last synced.
7. To open the content, select the document link next to **Sync with** in the **Policy text** field or select the **Open in Word** button in case of Microsoft OneDrive or the **Open in Google docs** button in case of Google Drive.
   - If you enable **Sync with**, then the document cannot be simultaneously edited both in the Cloud and in the **Policy text** field. The content can be updated in the Cloud and can be pulled into the **Policy text** field.
   - If you disable Sync with, then your policy text document content is disconnected from the Cloud document and you can edit the content independently. You can save this content by selecting the **Save** button.

     In the disconnected state, if one of the reviewers had updated the policy text and logging in as a policy owner if you select the **Complete publishing checklist**, then the **Attach policy as PDF** becomes a required step to attach the PDF.

     You must manually remove the previous policy attachments, if any, and confirm before you attach the current policy as a PDF in the playbook.

   You can also view the policy text in the Details related list. If you update the policy text in the Details related list, then the policy text is automatically updated in the **Policy text** field of the Policy text related list.

   For a policy that is redlining enabled or not

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- If you are a compliance user and if the policy is in the draft state, then you can edit the policy text.
- If you are an owner or a reviewer and if the policy is in the review state, then you can edit the policy text.

For redlining-enabled policy

In addition to the preceding conditions, you can also edit the policy text for a final review and correction after you complete the publishing checklist and before requesting approval and publishing.

You can then complete the publishing checklist, request approval, and publish the policy.

## Provide document access to policy users

Grant access to the users who have assigned roles to collaborate on the redlining-enabled policy.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst; mp_document_user

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the list icon ( ).
3. Navigate to **Compliance library** > **My policies**.
4. Select a policy to open.
5. To view all the users of this policy and their respective roles who can access the document, select the **Document access** related list.
   The **Document access** related list is visible only when policy redlining is enabled for the policy. The Document access [sn_irm_shared_cmn_document_access] table stores the created and updated information of the policy record whenever there were corresponding changes to the user roles such as approvers, contributors, reviewers, or owners who have access to the redlining-enabled policy.

   The users identified in the **Policy Assignment** section of the Details related list as Owners, Approvers, Reviewers, and Contributors are users listed in the Document access related list for the redlining-enabled policy. A user can also have multiple roles.

   The **Status** column reveals the status of access each user has on the policy.

   If the **Object ID** entered is valid, then document access is granted. As a policy owner, you can also select each user and submit their unique **Object ID** in the respective fields of the Submit ID pop-up.

   In case of Google Drive integration, the Email of the user configured in the sys_user table is used to validate the authenticity of the user and grant access to the document hosted in cloud.
6. To access the document in Microsoft OneDrive as a user, execute the Sync collaborators scheduled job as and when required.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To execute the job, see Sync collaborators. Executing this job is a pre-requisite for using this feature.

**Note:** Although users of Microsoft OneDrive are granted edit access, not all of them can edit the document. The edit access depends on the state of the policy.

- If the policy is in Draft state, the Owner and Contributors have edit access. The Approvers and Reviewers get read access only.
- If the policy is in Review state, the Owner and Reviewers have edit access to the document. Contributors at this state do not contribute to the policy and can only read the document. Approvers also have only read access.
- If the policy is in Awaiting approval, Published, or Retired states, then all users have read access only.

## Complete publishing checklist and request policy approval

Use the playbook available with Compliance Workspace to complete the publishing checklist before you request approval. If approvals are complete, then the policy is automatically published.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst; mp_document_user

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the list icon ( ).
3. Navigate to **Compliance library** > **My policies**.
4. Select the policy publishing checklist icon ( ) in the right panel.
   A playbook checklist is created.
5. Complete the activities as a policy owner in the playbook.

**Publishing policy playbook activities**

| Activity | Description |
|---|---|
| Finalize document | Complete the task of accepting or rejecting the track changes and removing open comments. To avoid having internal comments in the published policy and thereafter in the Knowledge Base article, you must clean up the document.<br>**a.** Select **Open Document** to open the document and remove the comments.<br>**b.** After the document is auto-saved, select **Mark Complete** to mark the step as complete and to pull the updated content from Microsoft OneDrive or Google Drive account to this section. |
| Review formatting | Review the formatting of the text in the **Policy text** field before it's published as Knowledge Base article and select **Mark Complete**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Activity | Description |
|---|---|
| Review attachments | Review the existing policy attachments and remove documents that are outdated. You can also add new attachments to the policy at this stage. |
| Attach policy as PDF | Attach the policy document as a PDF to the Knowledge Base article. Attaching a PDF is recommended if your Microsoft OneDrive or Google Drive document and the **Policy text** field aren't in sync.<br>**a.** Select **Attach** to append the PDF to the policy.<br>**b.** Select **Mark Complete**. |
| Review Publishing settings | Refresh the browser after completing this step. Update the policy Knowledge base and the Policy template fields if necessary, and mark the step as complete. |

The **Complete publishing checklist** button is no longer available.

6. To view your attachments, select in the right panel.
7. Select the **Request approval** button to request approval for the policy.
8. Select **Approvers** in the Request approval pop-up.
9. Select **Request**.
   The policy moves to the **Awaiting approval** state.

   The policy approver can view the policy by navigating to the Approvals related list of the policy. Based on the approver's action, the policy either gets approved or rejected. If rejected, the policy moves back to the Draft state.
10. To edit a published policy, select the **Edit policy** button.

## View the history of a redlining-enabled policy

Use the policy history related list to track the modifications made to the policy document.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_analyst; mp_document_user

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the List icon ( ).
3. Navigate to **Compliance library** > **My policies**.
   You can create a new policy or open a record to enable the redlining feature.
4. Select a policy to open.
   If the policy is already published and requires a review, then reopen the policy for the review and approval process.
5. To update the published policy, select the **Edit policy** button.

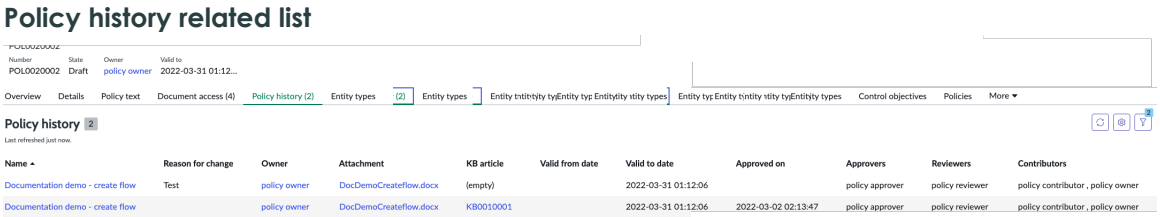
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Enter a reason for updating the policy in the **Reason for edit** field of the Edit policy pop-up.

b. Select the **Edit** button.
Edit policy action moves the policy back to the Draft state and opens it for yet another round of review and approval processes. When this cycle is complete and the policy is published, another record is created in the policy history.

6. Select the Policy history related list.
The history of the policy document with the basic information such as the name of the policy, reason for change, policy owner, the latest version of the policy text as an attachment, the validity period of the document, the approvers, reviewers, and contributors of the document are added when the policy is created. However, the Knowledge Base article is created only after the policy is published. So is the **Approved on** field updated when the approvers approve and the policy is published.

The records are added and are maintained in the policy history list whenever there's a change made to the policy and reviewed, approved, and republished.




You can view the entire history of the corrections and modifications made to the policy document from the time it was created. Update the policy document periodically to keep the policies current and up to date with the changing business processes. Maintaining a history of the policy document helps organizations track the next review cycle according to the changing business needs.

## Set up the dynamic approval configuration on a policy record

A policy is a set of guidelines and rules established by a business organization to govern its operations. Creating an approval configuration record for a policy enables you to define one or more approval levels and approval rules based on various dynamic conditions.

Beginning with the Utah release, you can set up the dynamic approval configuration on a policy record. The policy table consists of the policy records that regulate the status of the policies. Before implementing a policy, it goes through a review and approval process.

Setting up the dynamic approval configuration on a policy record enables you to define multiple levels of approvals based on various dynamic conditions such as policy type, state, and owner that are related to the policy fields. When you set up the dynamic approval configuration on a policy record, the approvers for a policy are added dynamically to the policy record.

### Limitations of adding the approvers manually

The existing approval configuration process uses the manual approach that has the following limitations:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The approval configuration process uses a single level of approval. If multiple levels of approval are not used, it increases the possibility of introducing errors and oversights in the approval process.
- The approvers for a policy cannot be changed based on dynamic or changing conditions of the approval process.
- The approvers are added manually to the record. The process can be time consuming, especially in large organizations or complex decision-making structures.
- Adding the approvers manually can lead to significant delays. Waiting to receive all approvals can slow down the decision-making process and decrease productivity.

## Benefits of dynamic approval configuration

Setting up the dynamic approval configuration on a policy record offers the following benefits:

- Organizations often encounter dynamic and changing environments. Having the flexibility to change the approvers allows the approval process to adapt to shifting circumstances. It ensures that the most appropriate individuals are involved in the approval process at any given time.
- For complex or high-stake decisions, configuring multiple levels of approvals enables the reviewers to conduct a comprehensive review of relevant factors. It ensures that the decisions are not rushed and that the potential impacts are carefully assessed for different scenarios.
- Changing the approvers dynamically can streamline the approval process and reduce the administrative overhead, thereby saving time and resources.

## Use cases for requesting multiple levels of approvals

Approval configuration can help create complex approval levels without manually adding approvers for each policy. In some cases, a policy owner may want to conduct multiple levels of approvals for a policy. For example, a policy is related to the HR domain. The compliance team, legal team, and HR team want to review and approve it. The policy owner can assign the HR team as Level 1 approvers of the policy.

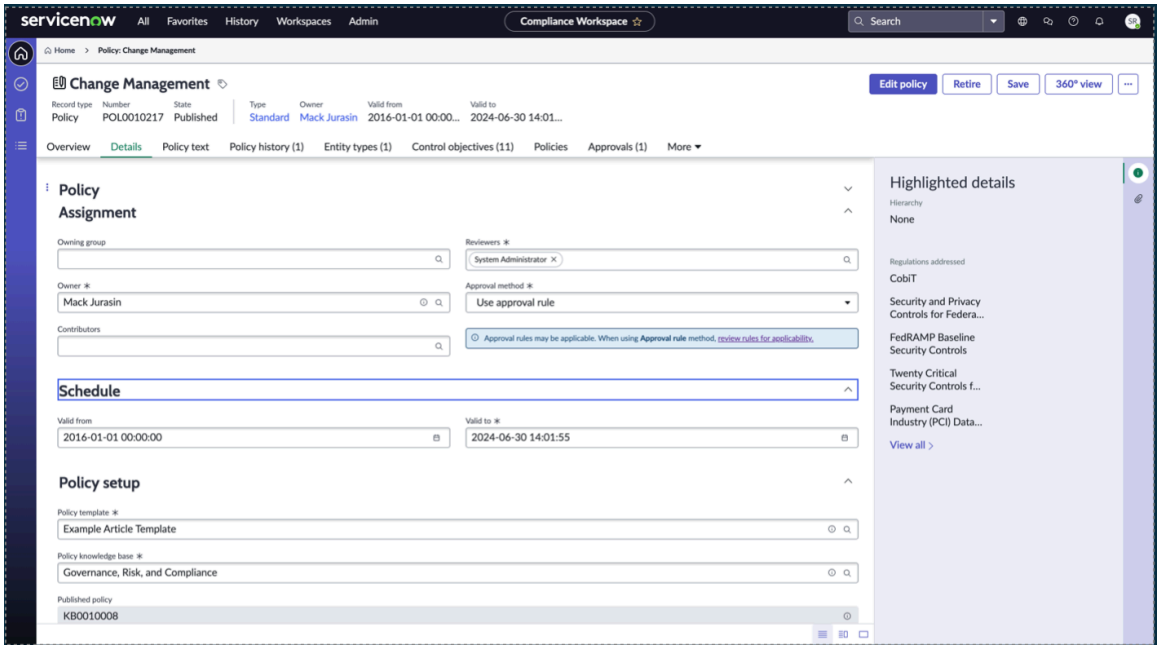
When the HR team approves the policy, it is assigned to the Compliance team for Level 2 approval. It is then assigned to the legal team for Level 3 approval of the policy. Also, the policy owner may want to select the approvers dynamically based on certain rules that match with the policy.

This use case highlights the importance of integrating dynamic approval configuration with a policy and configuring the policy approval rules with Approval Configurator.

## Approval configurator

To use the approval configuration, the approval method on the policy should be selected as **Use approval rule** as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




Approval configuration should be created for the policy and valid approval rules should be configured for the users.

In the Compliance Workspace, you can navigate to **Policy and Compliance** > **Policies and Procedures** >**Policy Approval Rules** to configure the approval rules.

## Configuring policy approval rules using Approval Configurator

You can set up various approval rules using the Approval Configurator:

- Set up multi-level approval rules based on dynamic conditions.
- Send approvals to a user or a group of users selected from a field from the source record or select the user or groups manually.
- Set up only one approval or all approvals as required approvals.

To set up approval configuration on a record, see the following sections.

1. To set up an approval configuration record, see Set up approval configuration.
2. To assign an approval level for the approval configuration record, see Set up approval levels.
3. To set up an approval rule for the approval level in the approval configuration record, see Set up approval rules.

### Note:

For more information on the roles in the GRC: Approver Configurator application, see Roles installed with GRC: Approver Configurator.

## Roles required for creating policy approval rules

To create the policy approval rules, the following roles are required:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- A user with the sn_compliance.manager role can create policy approval rules with the sn_grc_appr.admin role.
- Users with the sn_grc.business_user and sn_grc.business_user_lite and above roles can view a policy.
- A user should have mp_document_user with either the sn_grc.business_user or sn_grc.business_user_lite role to access the document when redlining is enabled.

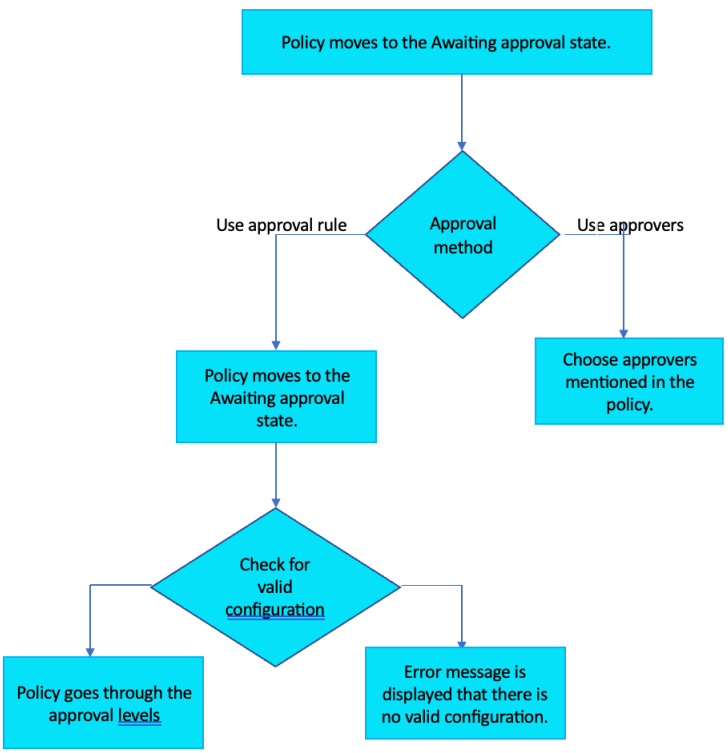
## Workflow for setting up approval configuration

When you set up approval configuration on a policy record, the workflow contains the following steps.

1. When an approval is requested for a policy record, the state of the policy changes to the **Awaiting approval** state.
2. If the approval method is selected as **Use approvers**, it uses the approvers mentioned in the policy record.
3. If the approval method is selected as **Use approval rule**, it checks for a valid configuration that suits the policy record. The dynamic approval configuration searches for the approval configuration record that is related to the policy.
4. The dynamic approval configuration then retrieves the approvers from each approval level record and sends an approval request for each level.
5. If a valid configuration is not found, an error message is displayed that there is no valid configuration for the policy.

The workflow steps are shown in the following example.

**Workflow for setting up approval configuration**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

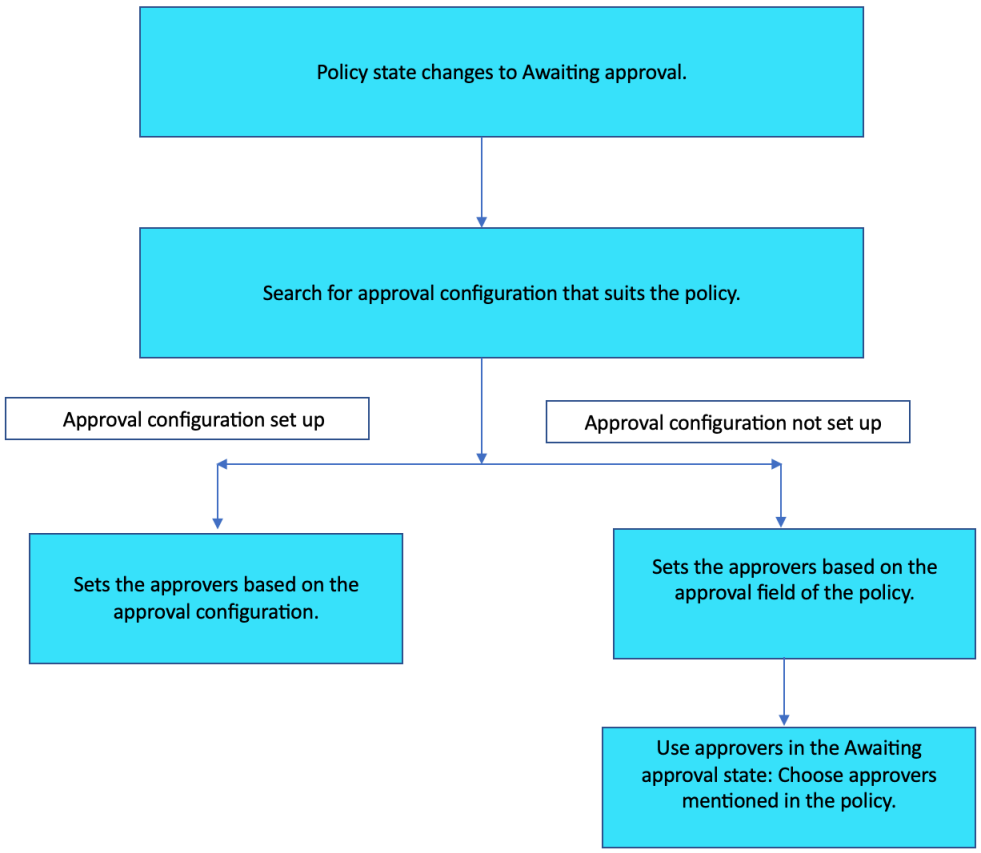
If you are the policy owner, you can select the approvers for the policy in the **Approvers** field of the Policy form. The approvers are usually the users who have the Compliance User role. If you do not have proper access, you cannot access the policy record. To request access to the policy record, you must contact the Compliance Administrator.

## Integrating dynamic approval configuration with a policy

To integrate dynamic approval configuration with a policy record, you can set up multiple approval levels and for each level, you can set up the approval rules. Based on the approval levels and rules setup, the approvals are triggered automatically. When one level is approved, the policy record is submitted for the next level of approval.

The workflow for integrating dynamic approval configuration with a policy is shown in the following example and steps.

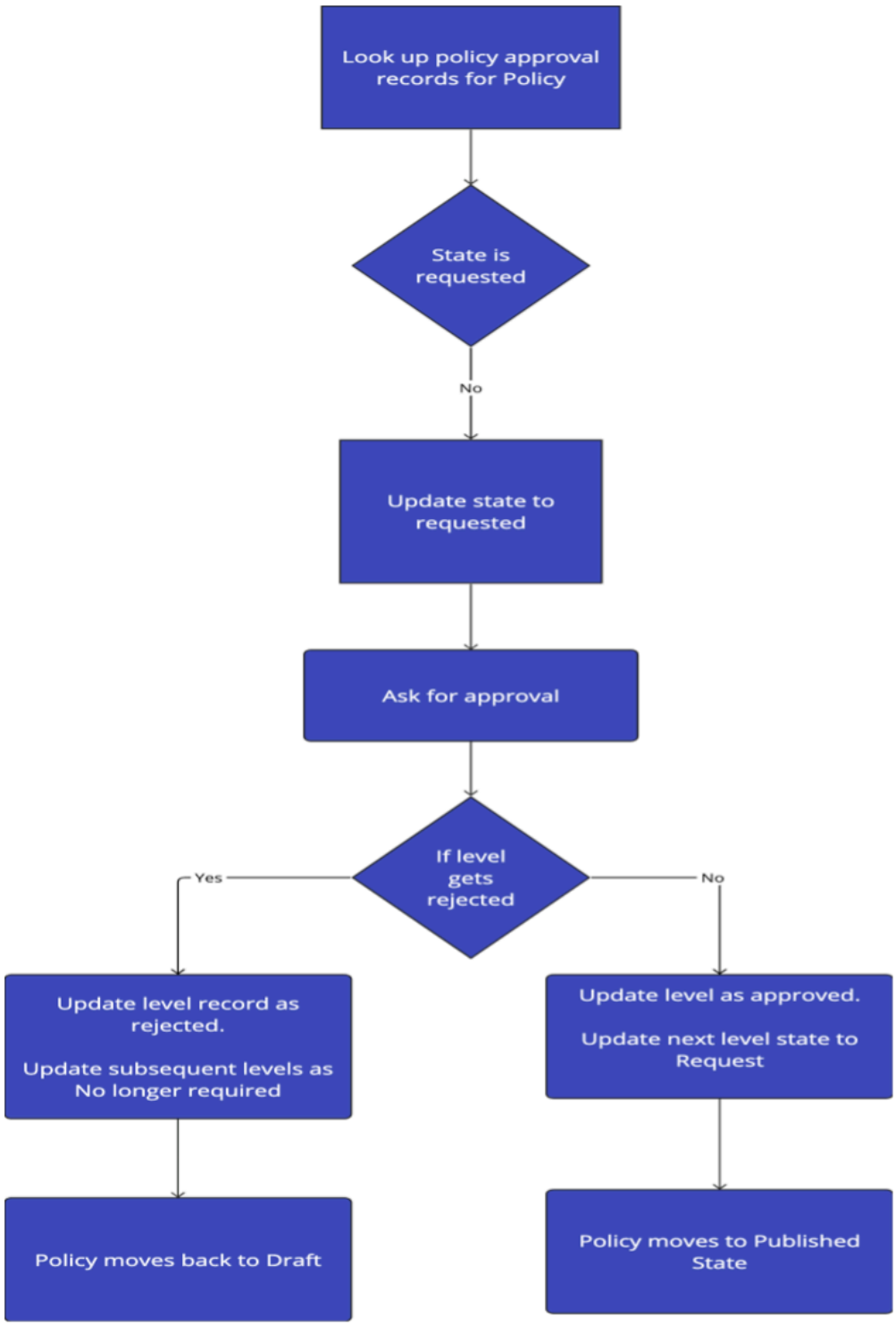
**Integrating dynamic approval configuration with a policy**




- When an approval is requested for the policy, the state of the policy changes to the **Awaiting approval** state.
- The dynamic approval configuration searches for the approval configuration record that is suitable to the current policy.
- If dynamic approval configuration is not set up on a policy record or even though it is set up, it is not applicable to that particular policy record, an error message is displayed that no valid configuration is found for the policy record and the record gets aborted. Users have to go back to your policy record and select the approvers or create a valid configuration for the policy record.
- If dynamic approval configuration is set up, the approvers, approval levels, and rules are added based on the configuration of the approval configuration record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The complete workflow is shown in the following example.




## Components used for dynamic approval configuration

The following components are used for setting up the dynamic approval configuration on a policy:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The Policy approval rules module creates or checks the approval configurations with the source table as policy.
- The Policy approval table stores the approvers of each level of the approval configuration. It can be used for tracking the status of the approval levels.
- Based on the current level decision, the policy either gets forwarded to the next level of approval or if it gets rejected, it is reset to the **Draft** state. If all levels are approved, the policy moves to the **Published** state.

## Configure dynamic approval configuration on a policy

Set up dynamic approval configuration on a policy. Based on the configured approval levels, the Policy and Compliance Management application configures one or more approval rules on the policy record.

### Before you begin

Role required: sn_compliance.manager, sn_compliance.user

### About this task

A user with the sn_compliance_ws.corporate_compliance_manager role can create dynamic approval configuration and a user with the sn_compliance_ws.corporate_compliance_user role has read permission for the policy record.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the List icon.
3. Navigate to **Compliance library** > **My policies** and select **New**.
4. Enter the name of the policy.
5. In the Policy Assignment panel, update the **Owner** and **Reviewers** fields.
6. Select the approval method in the **Approval method** field.

| Step | Description |
|---|---|
| **Select approvers** | Option to select the approvers on the policy record. You can add the approvers in the **Approvers** field. |
| **Use approval rule** | Option to use the approval rule for dynamic approval configuration. Based on the set-up of the approval configuration and configured approval levels, the system applies one or more approval rules on the policy record. Once an approval rule has been configured, that value is populated in the **Approval rule** field. |

For more information on creating a policy in the Compliance Workspace, see create a new policy.

**Note:** If dynamic approval configuration is not set up on the policy record, the approvers are added in the **Approval** field of the policy.

7. In the Schedule panel, update the date for the record in the **Valid to** field.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Select **Save**.
9. Select **Request approval**.

   The policy owner can request approval and complete the workflow on the policy record. For a given approval configuration on the policy record, the system applies the configured approval rules dynamically at each approval level. Once the **Awaiting approval** state is triggered and the **Use approval rule** option is selected as the approval method, the field gets populated with the details such as the configuration being used for the approvers.

   If the policy gets rejected at any level, it is reset to the **Draft** state. When all levels are approved, the policy moves to the **Published** state.

## Configure dynamic approval configuration on a policy with redlining enabled

Set up dynamic approval configuration on a policy for which redlining is enabled.

### Before you begin

Role required: sn_compliance_ws.corporate_compliance_manager, sn_compliance_ws.corporate_compliance_user

### About this task

A user with the sn_compliance_ws.corporate_compliance_manager role can create dynamic approval configuration and a user with the sn_compliance_ws.corporate_compliance_user role has read permission for the policy record.

To use dynamic approval for policy redlining, ensure that the redlining setup is done and the users in the approver rule have required roles for document access. When redlining is enabled, a user should have the mp_document_user role with either the sn_grc.business_user or sn_grc.business_user_lite role to access the documents.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, select the List icon.
3. Navigate to **Compliance library** > **My policies** and open a policy record.
   You can create a new policy or open a policy record to enable the redlining feature.
4. Select the Policy text related list to view the contents of the policy text.
   a. Select the **Enable Word editing** button.
   b. To create a document as a policy owner, select **Create new document** in the **Enable Word editing** list.
   c. Enter the path to the Folder including the Folder name in the **Folder link** field in the Create a document pop-up.
   d. Enter the name of the document in the **Document name** field.
   e. Select **Create**.
5. Select the **Request review** button.
6. Select **Request**.
7. Select the **Complete publishing checklist** button.
   You can complete the tasks in the publishing checklist. For more information on redlining, see Policy authoring and redlining in Compliance Workspace.
8. Select **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. Select **Request approval**.

   If an active dynamic approval configuration does not have any users associated with it, it is not considered as a valid configuration. In such cases, selecting **Request approval** returns an error message: `Could not request approvals because matching approval rule could not be found. Make sure to configure appropriate approval rule for this policy here.` To rectify the error, edit the configuration and request approval again.

   The **Document access** tab displays the revised list of the users who can access the policy as described in the following example:

   a. When the policy first moves to the **Awaiting approval** state, approval configuration is applied on the policy record. If the policy has two levels of approval, the document access is provided only to level 1 users by default. Group users of level 1 can get access through the **Request document access** UI action.

   b. Once level 1 users approve the policy, the document access is added for level 2 users. If any user rejects the policy at level 1, it moves to the **Draft** state.

   c. When the policy moves to the **Awaiting approval** state again, next level of approval configuration (for example, approval configuration 2) is applied on the policy record. In this case, all users that are common between the two levels and have access to the document, can access the policy and the document access is removed for the rest of the users.

   The **Request document access** UI action is visible to the users with the business user role and business user lite role. If any user groups do not have these user roles, they cannot access the document. The approvers have the view access or comment access in the approval state.

   > **Note:** In the approval rule, the access is given to the individual users only and not to the group users. Giving access to many users in the group can lead to performance issues.

   If you are a group user, you must select **Request document access**. The group users can log in as one of the users in the group and select **Request document access**. The group users are then granted the document access and a message is displayed: `Doc access request has been raised, please refresh or try to access document in a few minutes.`

   In the approval configuration workflow, if an approver rejects the policy at any level, it moves to the **Draft** state. The **Document access** tab in the form displays a list of the users who have access to the policy with the roles and status displayed. Only level 1 users can access and review the record. When level 1 users approve the record, then the document access is provided to level 2 users, and so forth.

   When all levels are approved, the policy moves to the **Published** state.

10. In the **Policy text** tab, select **Open in Word**.

    The Word document opens up in the tab. In the **Manage access** tab of the document, you can also view the users who have permissions to view the document. The configured policy approval rule is displayed in the **Approval rule** field. The Approval levels related list displays information on the approval levels, users, and status of the approval for the policy record.

    If the policy gets rejected at any state, it is reset to the **Draft** state. Once the approvers approve the policy, it moves to the **Published** state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

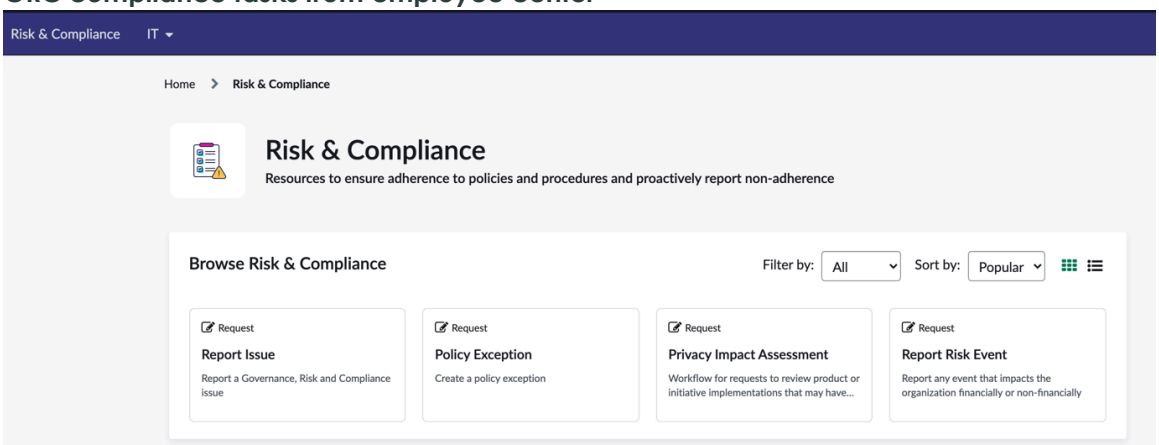
# Managing GRC tasks from Employee Center

Employee Center is designed for enterprise services based on employee needs. The employee center is also called as Business user service portal as the portal is exclusively for GRC business users to request an issue triage or raise a policy exception.

You can use Risk and Compliance section of the Employee Center to manage some of the common compliance tasks like triage issues, raise policy exceptions, and GRC assessments.

You can view all the tasks that are assigned to you if you login as a user with GRC business user role.

### GRC compliance tasks from employee center




## Report a GRC issue from Employee Center

Use the employee portal to review and work on the action plan related to the observation which is confirmed as an issue that as an auditee or issue owner you need to remediate.

### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

**Note:** If you have installed GRC: Advanced Core, then by default the value of the *sn_grc_advanced.enable_my_issues_hide_my_reported_issues* system property is also set to **true**. These two conditions must be fulfilled to view the Issue triage form in Employee Center. Otherwise, you can view only the Issue form.

### About this task

Use the Report Issue form to report an issue based on a control breakdown, missing policy, or an event that is non-compliant to a policy, standard, guideline, or regulation. You can also use this form to suggest an improvement or to report a risk event.

### Procedure

1. Navigate to **Self-Service** > **Employee Center**.
2. Select the **Risk & Compliance** section.
3. Select the **Report Issue** catalog item.
4. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Report Issue form**

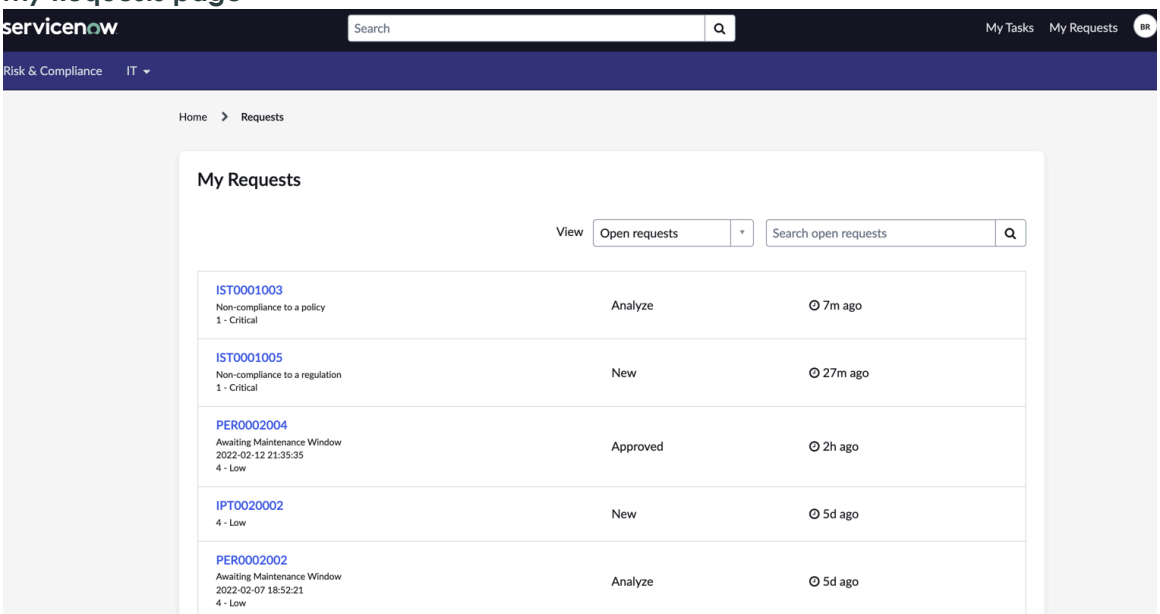
| Field | Description |
|---|---|
| What is the issue? | Brief description about the issue. |
| Describe in detail | Detailed description of the issue. |
| When did you discover the issue? | Date the issue was identified. |
| What is the issue related to? | Entity to which the issue is related. |
| What was affected? | Record details of the entity that you selected.<br><br>The options in this field depend on the entity that you select in the previous field. |
| What type of issue is this? | Type of issue. |
| Other | Option to select if you do not find the correct category of entity to which your issue is related.<br><br>Following four fields appear if you select the **Other** option. |
| Has the incident already occurred? | Indicate whether the incident has occurred before. |
| Was there a monetary loss? | Monetary loss associated to the issue. |
| Currency | Currency in which the loss is estimated.<br><br>If there was a monetary loss, then this field appears. |
| What is the expected monetary loss? | Estimated monetary loss as a result of the issue. |
| Select the impact rating | Non-monetary impact of the issue. The choices are as follows:<br>◦ **Low**<br>◦ **Medium**<br>◦ **High** |
| How was the event discovered? | Source through which the issue was identified. |
| What actions have you taken so far to contain or remediate the issue? | Brief description of the action taken to remediate the issue. |
| What do you believe to be the root cause of this issue? | Analysis of the root cause of the issue. |

5. Select **Submit**.
   You are directed to the My Request summary page where you can view your issue triage request number. This page is read-only and you can view all your requests that you have raised as a business user.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Post a message in the **Activity** field to prioritize your issue when it is being triaged.
7. Select the **Attachments** tab to attach any document related to the issue.
8. Click **My Requests** link at the top right corner to view all the requests that includes your issues and issue triage.

**My Requests page**

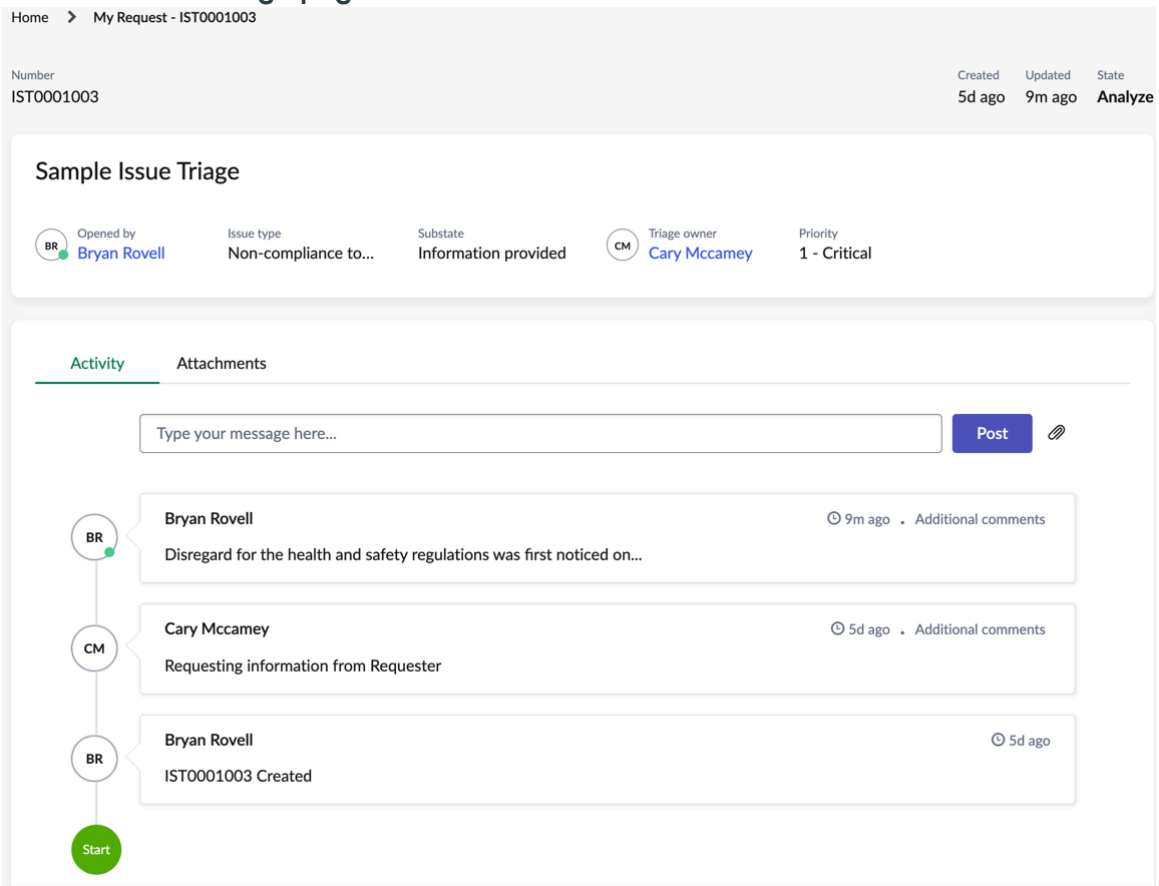



9. Click the issue triage request number, which has a prefix IST, to view messages, if any, from the approver.
   The issue triage list view header displays the name of the person who opened the issue triage, issue type, substate, triage owner, and its priority.
10. To send additional information on the issue triage to the triage owner, click the **Actions** list.
11. Enter your information in the **Comments** field of the Send additional information pop-up.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

12. Click the **Send** button.

**List view of issue triage page**




## Create a policy exception from Employee Center

Use the Employee Center to request exceptions for policies, control objectives, controls, or issues by specifying the reason of exception on a particular list of the systems, applications, networks, or entities for which the exception applies.

### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

### Procedure

1. Navigate to **Self-Service** > **Employee Center**.
2. Select the **Risk & Compliance** section.
3. Select the **Policy Exception** catalog item.
4. On the form, fill in the fields.

**Policy Exception form**

| Field | Description |
|---|---|
| What is the exception for? | Type of policy exception that you want to create. The options are: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ Policy: Create a policy exception based on a policy.<br>◦ Control objective: Default is a single control objective on which the policy exception is created.<br>◦ Controls: Option to create a policy exception on multiple controls.<br>◦ Issue: Option to create a policy exception on an issue. |
| Policy | Policy associated with this policy exception. |
| Control objective | Control objective associated with this policy exception.<br>When you select a control objective, the**Impacted controls** field appears. |
| Control | Select **Control** to associate multiple controls from different control objectives. This option supports multiple controls objectives for your policy exception, instead of creating multiple policy exceptions that could be applied on multiple controls. |
| Issue | Issue associated with this policy exception. |
| Impacted controls | Controls associated to the control objective. |
| Short description | Brief description about the policy exception request. |
| Description | Detailed description of the policy exception request. |
| Reason | Reason for the exception |
| Justification | Evidence or rationale for the policy exception. |
| Risk description | Description of the risk as performed by the risk manager during risk assessment. |
| Valid from | Day on which the policy exception begins. |
| Valid to | Day on which the policy exception ends. |
| Priority | Approval priority of this policy exception. |
| Watch list | Users that are notified when the request is updated. |

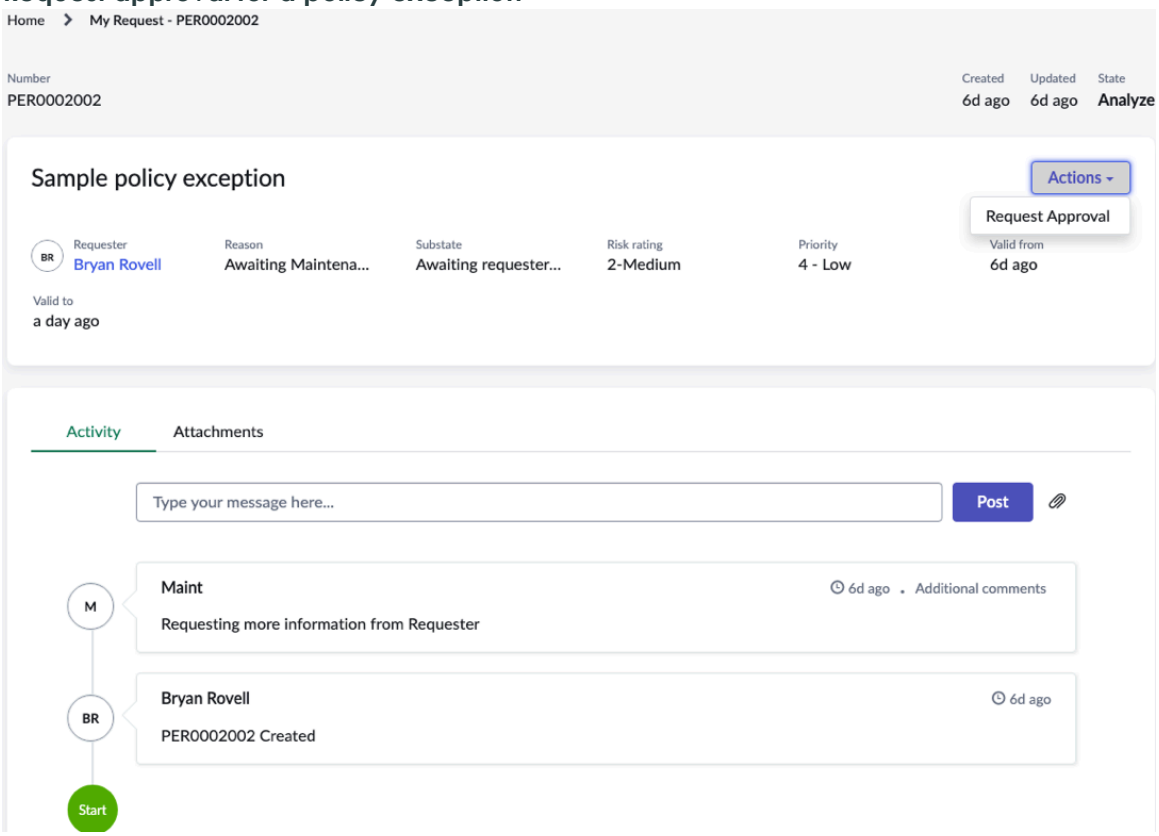
5. Click **Submit**.
   You are directed to the My Request page where you can view your policy exception number for the submitted policy exception request. This page is read-only and you can view all your requests that you have raised as a business user.
6. Post a message to support the policy exception in the **Activity** field.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. To attach a document related to the policy exception, select the **Attachments** tab.
8. Click **My Requests** link at the top right corner to view a list of all your requests that includes your issues and policy exceptions.
   The list shows 15 requests at a time. Click **Show More Requests** for more requests to be listed.
9. Select **Request Approval** from the **Actions** list if the request is in **Analyze** state.

   If you raise a policy exception from Employee Center and if verification rules are not configured, then the policy exception moves to the Analyze state. However, if verification rules are configured for the policy exception, then the policy exception moves to the New state and the verification approval process is triggered. As verification rules are configured the approver is required to verify the policy exception and approve it, only then the policy exception moves to Analyze state.

**Request approval for a policy exception**




10. After the policy exception is approved, you can request extension of your policy exception, select **Request extension** from the **Actions** list.

    a. Enter the new extension date that is later than the current **Valid to** date.
    By default, you cannot extend your policy for more than 30 days from the **Valid from** date. However, the extension can be relaxed based on the maximum exception duration days of the policy.

    b. Select a reason for extension from the list in the **Extension reason** field.

    c. Enter a justification for the extension.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

d. Click **Request**.
The number of remaining extensions that you can avail to request is displayed as **Remaining extensions**.

## Complete control assessments from the Employee Center portal

Use the Employee Center Home page to view all your requests, raise issue requests and policy exceptions, and complete all your GRC assessments.

### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

### About this task

You can manage all your pending tasks that are open by selecting the GRC tasks link. By default, you can view all the Indicator tasks that are assigned to you and in Open state. To view the indicator tasks in other states, select the filter icon next to the **State** column.

From this page, you can navigate to manage all your active items that include all GRC assessments, such as Control attestations, Risk assessments, Risk identification questionnaires, and Privacy assessments.

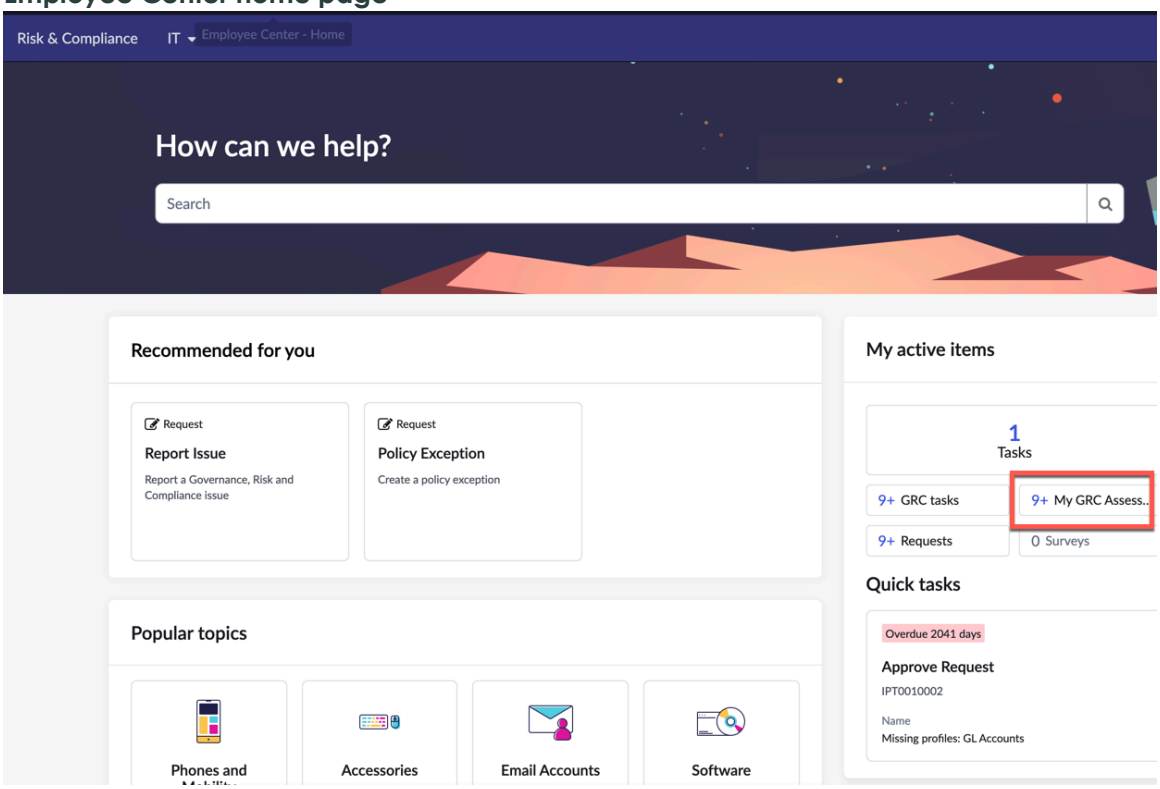
**Note:**

The **Risk identification questionnaires** tile is available only if GRC: Advanced Core plugin is installed.

### Procedure

1. Navigate to **All** > **Self-Service** > **Employee Center**.
2. Select **My GRC Assessments** in the **My active items** pane of the Home page.

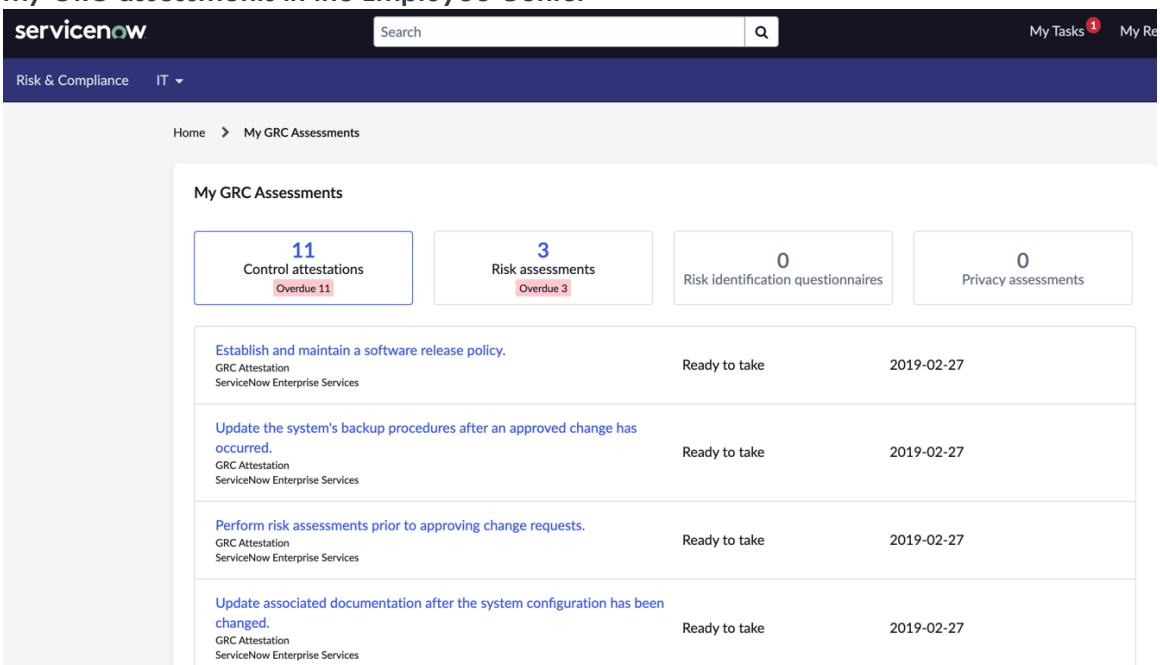
**Employee Center home page**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Control attestations tile is highlighted listing all your attestations that are active and due. It also displays the number of control attestations that are overdue and they're enlisted first in the list.

**My GRC assessments in the Employee Center**




There's a pagination limitation of displaying only 15 items at a time.

3. Select **Show More Requests** to display more requests.
4. Select the control attestation item in the list that you want to attest.
   The header displays the control objective, an entity that the control attestation belongs to, and its description.
5. Select the **Get Started** button.
6. Complete the attestation, providing an attachment and explanation, and select **Submit**.

## Policy knowledge base and quick links in the Employee Center portal

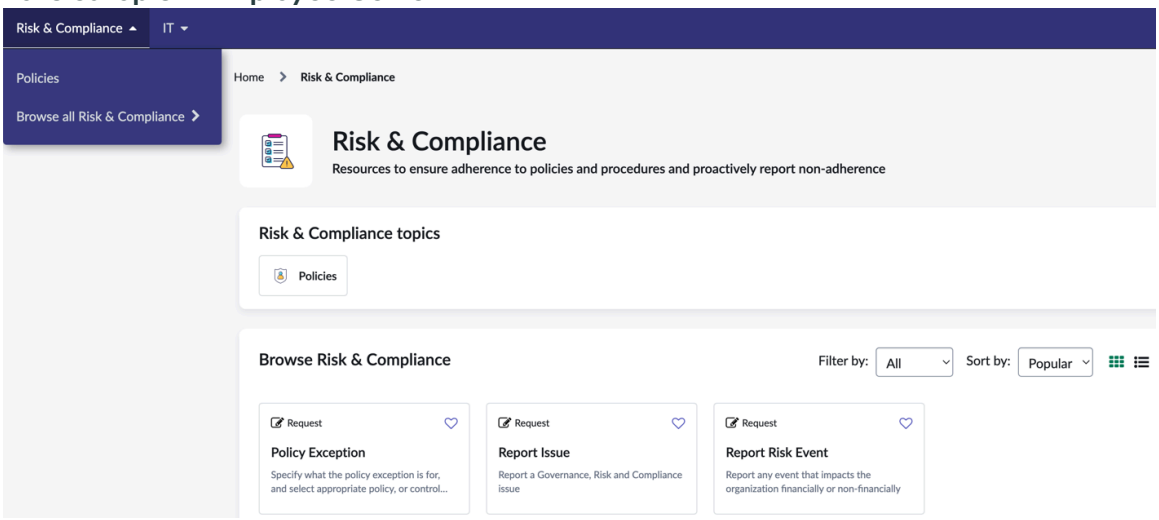
You can view all the Knowledge base (KB) articles related to the published policies in Employee Center.

Selecting the **Policies** option in the Risk & Compliance section takes you to the Policies page, where you can view all the Knowledge base (KB) articles that haven't expired yet.

**Note:** You can view all KBs even if the **Valid to** date is passed. However, when the policy retires, the corresponding KB will also retire, and such KBs will not appear.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

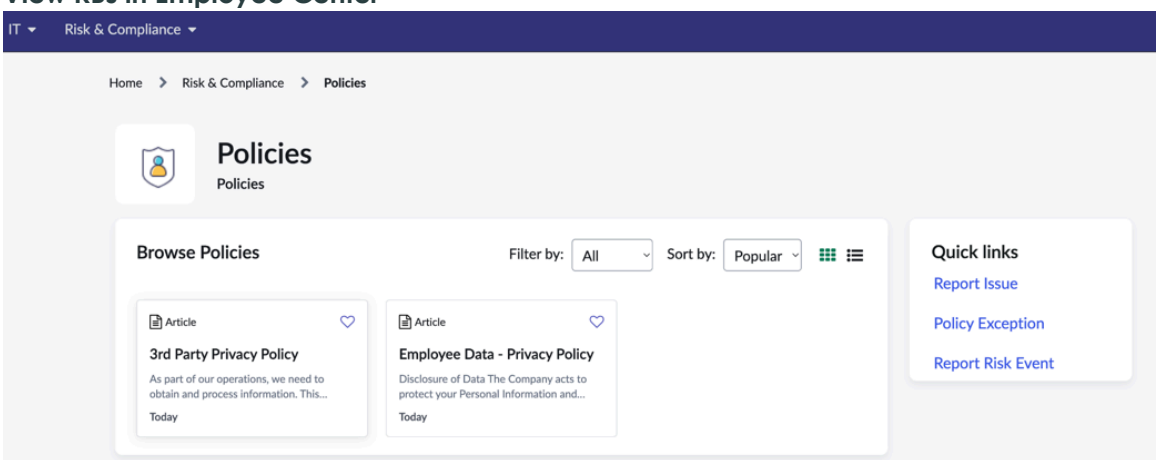
### Policies topic in Employee Center




The admin executes the scheduled job, *Pull the knowledge base articles related to policies*, on demand to pull all the KB articles of the published policies and list them in the Policies topic. The KBs of the published policies are listed in the policies page only when the scheduled job is run. Users with the business user or business user lite roles do have read access to the published KBs.

Access **Quick links** to the respective forms to create and accomplish your respective tasks. For example, to create an issue, select Report Issue link, enter the issue details, and submit it. Similar links are listed for quick access to report events and raise exceptions on policies with respect to Risk and Policy and Compliance, respectively.

### View KBs in Employee Center




## Group assessments for similar assessments in Employee Center

Group the assessments that have the same entity or control objective based on metric type, and additionally the same entity, control objective, or category to provide response to similar assessments.

### Before you begin

Role required: sn_grc.business_user, sn_grc.business_user_lite

### About this task

In Configurable Workspace, you can only group control attestations, and not risk assessments, vendor assessments, or privacy assessments. Such assessments and those assessments that can't be grouped by the selected **Group by** criterion are marked as invalid

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

and are displayed in the **Group previews** of the Group assessment pop-up, with a link to view such assessments.

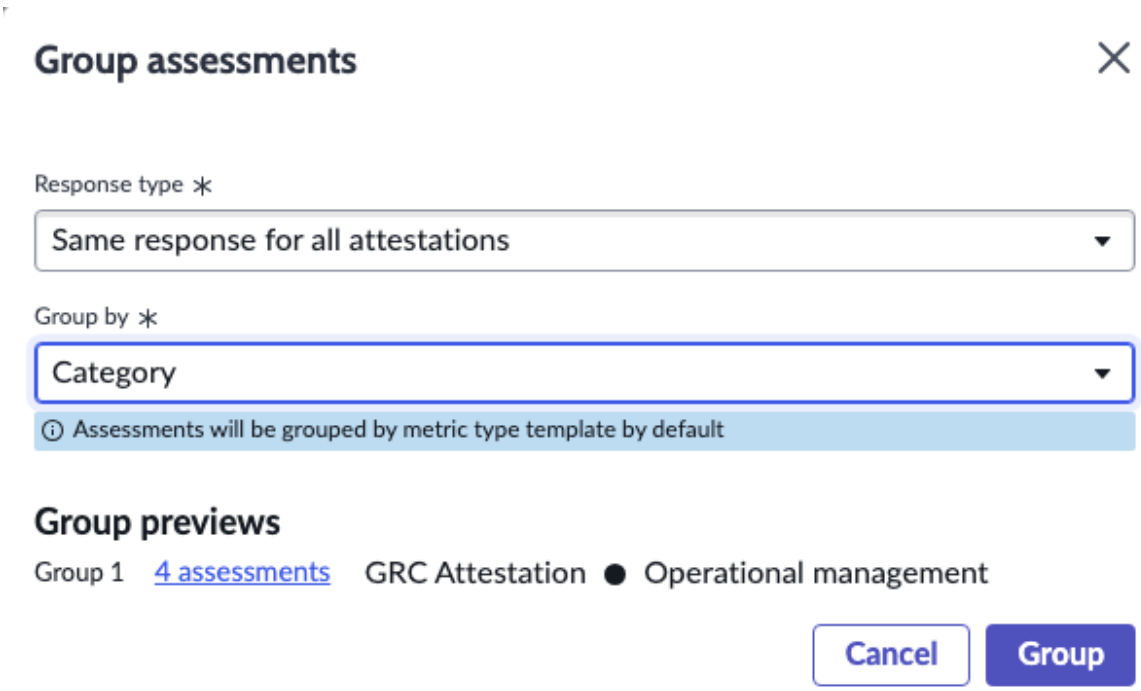
### Procedure

1. Navigate to **All** > **Self-Service** > **Employee Center**.
2. Select **GRC tasks** in the **My active items** pane of the Home page.
3. Select the Tasks icon on the left pane.
4. Select the attestation records in the list view of the Tasks page that you'd like to group.

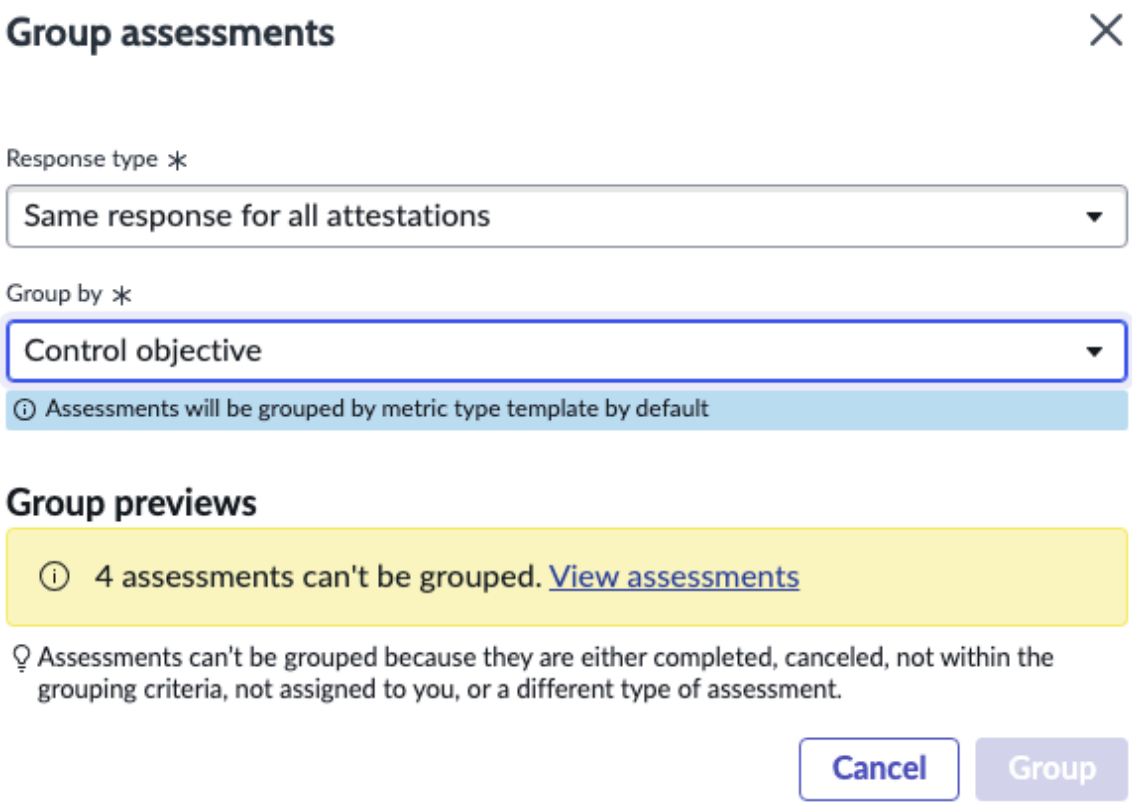
   **Note:** You must select at least two and can select up to a maximum of 13 assessment records for grouping.

5. Select the **Group assessments** button.
6. Select a **Response type** in the Group assessments pop-up.
   For more information on the response types, see Consolidate control attestations using the Same Response feature.
7. Select a criterion to group the assessments in the **Group by** list.
   By default, assessments are grouped by the metric type template. You can group the assessments by Category, Entity, or Control objective. If the selected assessments have a common category, entity, or control objective then they're grouped accordingly based on your selection. However, if the assessments selected do t have any of the common criteria by which they can be grouped, then the assessments are not grouped at all.

   The **Group previews** section displays the grouping details, assessments with links, and an appropriate message information if they're grouped or can't be grouped based on the Group by criterion, status, assignee, or the evaluation method of the metric type.



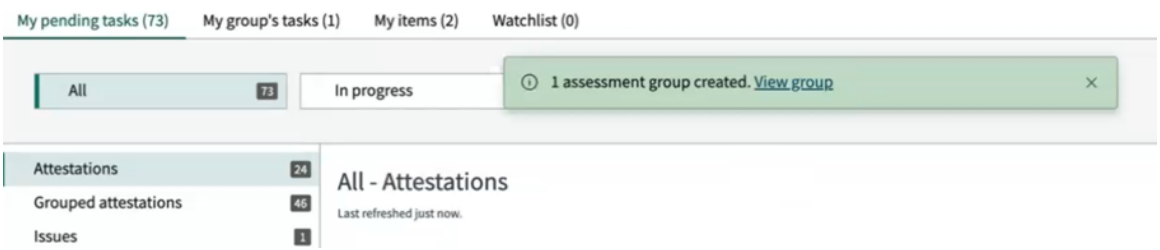

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




8. Select the **Group** button.
   If the grouping of assessments is successful, then you get a message indicating that the assessment group has been created, followed by a link to the grouped assessments.

   If a few of the assessments among the selected assessments couldn't be grouped by the selected criterion, then the **Group previews** pane displays the number of assessments that couldn't be grouped. Nevertheless, as there are other assessments in your selection that could be grouped by the selected **Group by** criterion, the **Group** button is active for you to select and group the rest, where the grouping is successful.

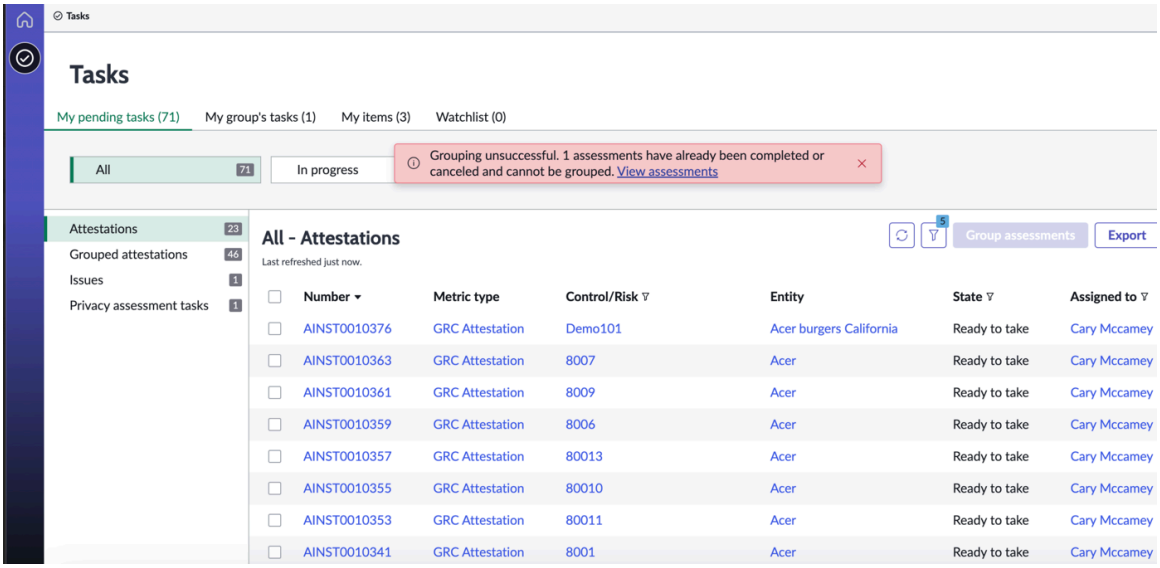
   On the other hand, if all the assessments that you selected are invalid, for example, risk assessments or privacy assessments, then the **Group** button is inactive as grouping isn't possible for such assessments.




**Note:** You can group the assessments that are in **Ready to take** or **In Progress** state, but not the assessments that are in **Complete** or **Canceled** state.

If the status of a record that you've selected for grouping has changed and is being assessed before you select the **Group** button to group the assessments, then such a record can't be grouped.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




9. Select the link to the grouped assessment in the UI message.
   The link takes you to the list view of the grouped assessments. Alternatively, you can also select the **Grouped attestations** on the left pane. The Assessment Instance page opens up, where you can take the assessment.

## 360° Relationship Visualization for Policy and Compliance Management

When you launch the 360° view from a particular compliance record, you can instantly explore the relationship between the selected record and all its associated objects in a distinctive visualization.

### 360° view

In Policy and Compliance Management, the 360° relationship view button is enabled in the following workspace forms:

- Authority document [sn_compliance_authority_document]
- Policy [sn_compliance_policy]
- Citation [sn_compliance_citation]
- Control [sn_compliance_control]
- Control objective [sn_compliance_policy_statement]

To explore the 360° view and for instructions to launch the view, see Exploring the 360° view.

To know more about the users who could use 360° Relationship Visualization, their roles, and responsibilities, see 360° relationship visualization.

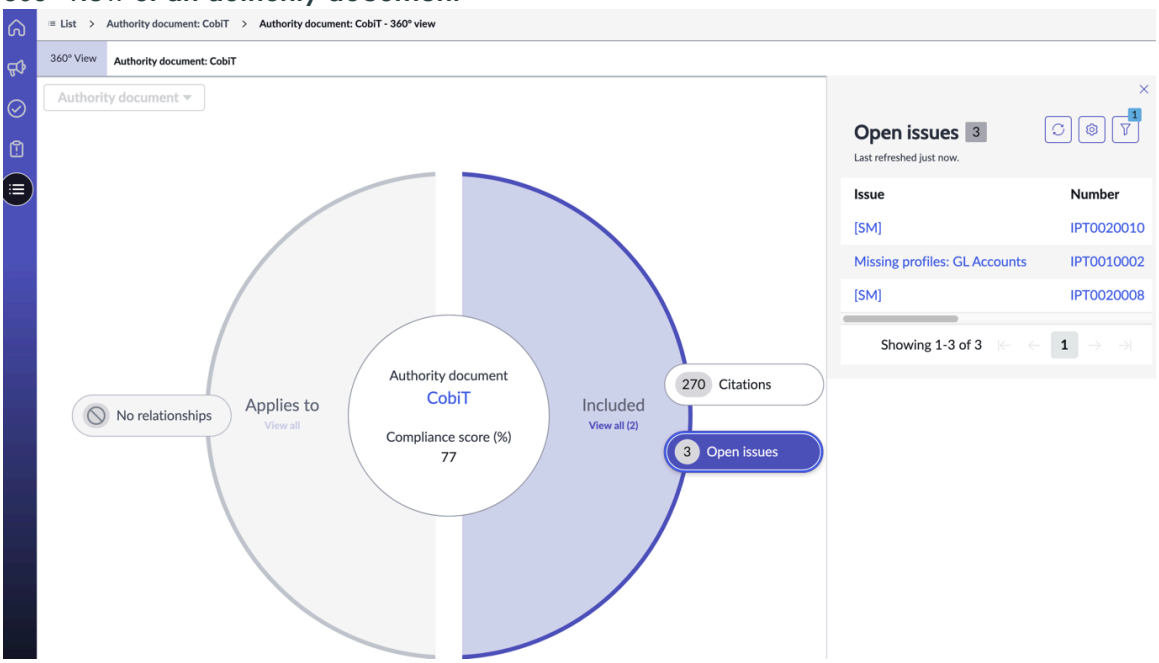
### 360° view of compliance objects integrating with issue in an m2m relationship

The 360° views from the compliance objects such as authority document, policy, control, control objective, and engagement in the Compliance Workspace give you a comprehensive and detailed overview of the issues that are linked to these objects in a many-to-many (m2m) relationship.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

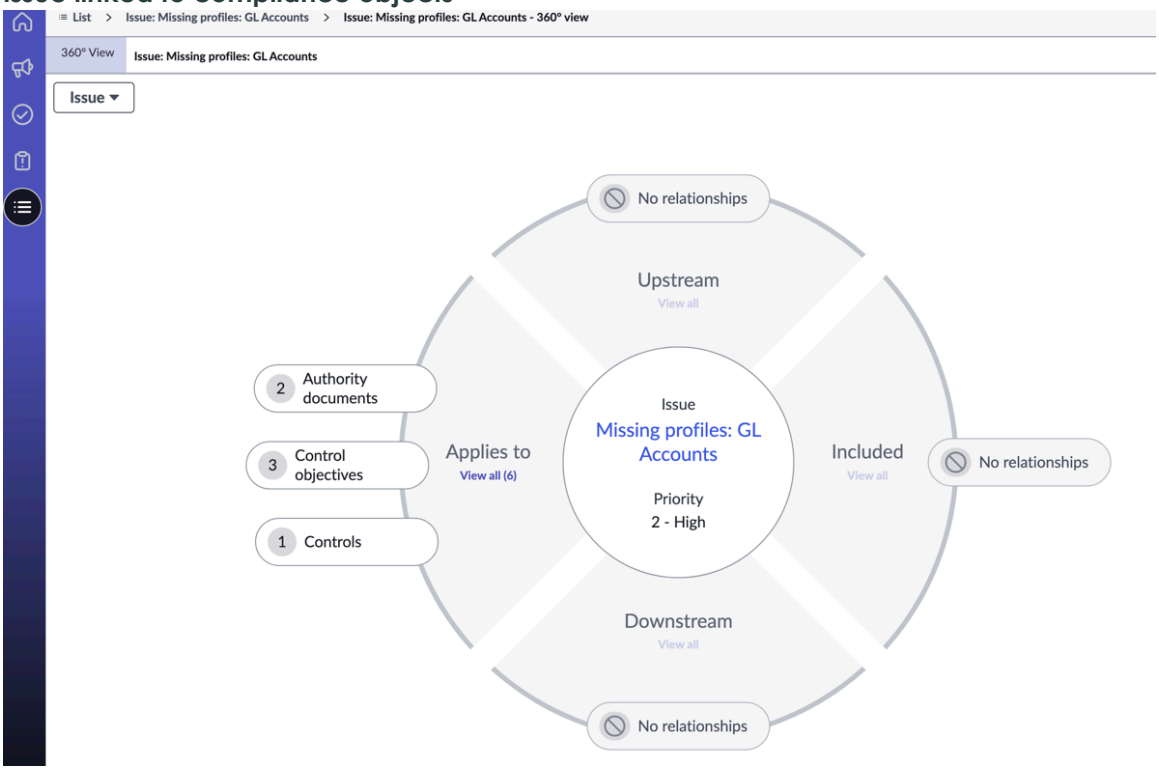
For example, clicking the **360° view** button from the authority document that is linked to an issue launches the 360° view enabling you to view the issues that are open for the authority document. You can get more details of the issues when you click the Open issues link.

### 360° view of an authority document




Similarly, you can navigate to the Issue's Overview page and click the **360° view** button. If the issue applies to any of the objects, or if it is linked to the objects in an m2m relationship, then the view gives you comprehensive integration details.

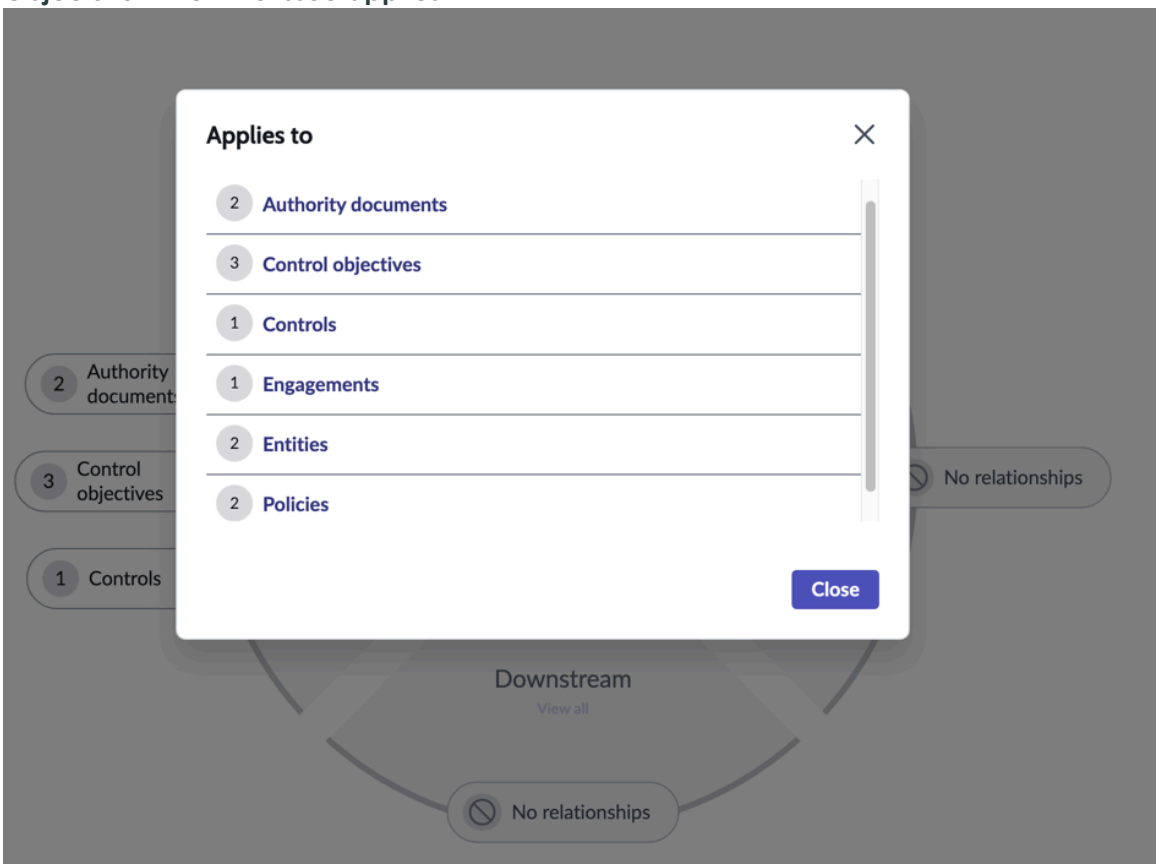
### Issue linked to compliance objects




You can click the View all link to view all the compliance objects that the issue applies to.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Objects to which the issue applies**




## GRC: Policy and Compliance integrator

The GRC: Policy and Compliance integrator application provides a common framework so that your content providers can push their content into the GRC applications. The application also enables you to review, approve, and import the data into the Policy and Compliance Management tables.

Starting in Utah, you can use the GRC: Policy and Compliance integrator application with the GRC: integrations with third-party content application.

For more information on how to complete the data import process, see Workflow for GRC: Policy and Compliance integrator and Using the GRC: Policy and Compliance integrator to display batch records and import tasks.

### Workflow for GRC: Policy and Compliance integrator

You can install the GRC: Policy and Compliance integrator application from the ServiceNow Store and execute the workflow to complete the data import process.

The GRC: Policy and Compliance integrator application workflow consists of the following steps:

1. Download the GRC: Policy and Compliance integrator application from the ServiceNow Store. When you download the GRC: Policy and Compliance integrator application, the GRC: integrations with third-party content and Policy and Compliance Management applications are automatically downloaded in your instance.
2. Log in with the sn_compliance.admin role into an instance and assign the sn_grc_cim.admin role to a user.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Use the APIs and staging tables that are supported with the applications and move the data from the staging tables into the GRC: Policy and Compliance Management application.

   For more information about how to integrate batch records and assign library import tasks with the GRC: Policy and Compliance Management application, see Using the GRC: Policy and Compliance integrator to display batch records and import tasks, Accessing the batch records in the content integration batch table, and Assign a library import task for approval.

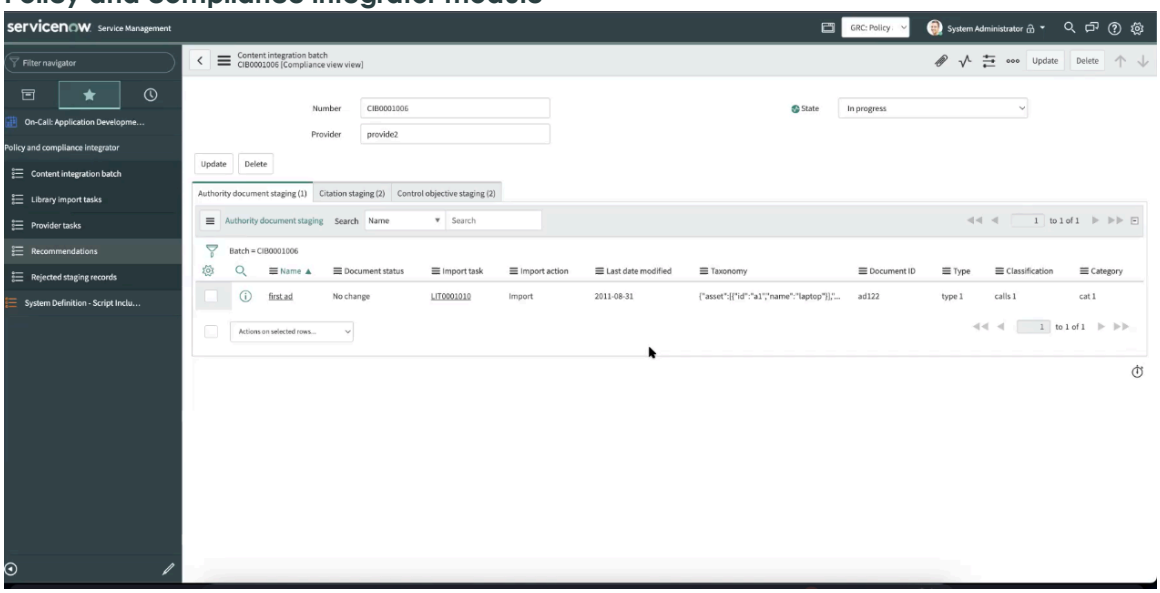
## Using the GRC: Policy and Compliance integrator to display batch records and import tasks

You can use the GRC: Policy and Compliance integrator application module to display the details of the batch records and to import tasks. For example, you can see the content integration batch records, library import tasks, staging records, and recommendations for the records.

You can access the GRC: Policy and Compliance integrator module by navigating to **All**>**Policy and compliance integrator**>**Content integrator** in the application UI. The module displays the following details that are shown in the following figure:

- Content integration batch
- Library import tasks
- Provider tasks
- Recommendations
- Rejected content

**Policy and compliance integrator module**




For information on how you can import the content from your third-party content providers into the Policy and Compliance Management application tables, see Accessing the batch records in the content integration batch table and Assign a library import task for approval.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Accessing the batch records in the content integration batch table

You can access the batch records in the content integration batch table that is displayed in the GRC: Policy and Compliance integrator application UI. By accessing these records, you can import the data into the Policy and Compliance Management application.

## Overview

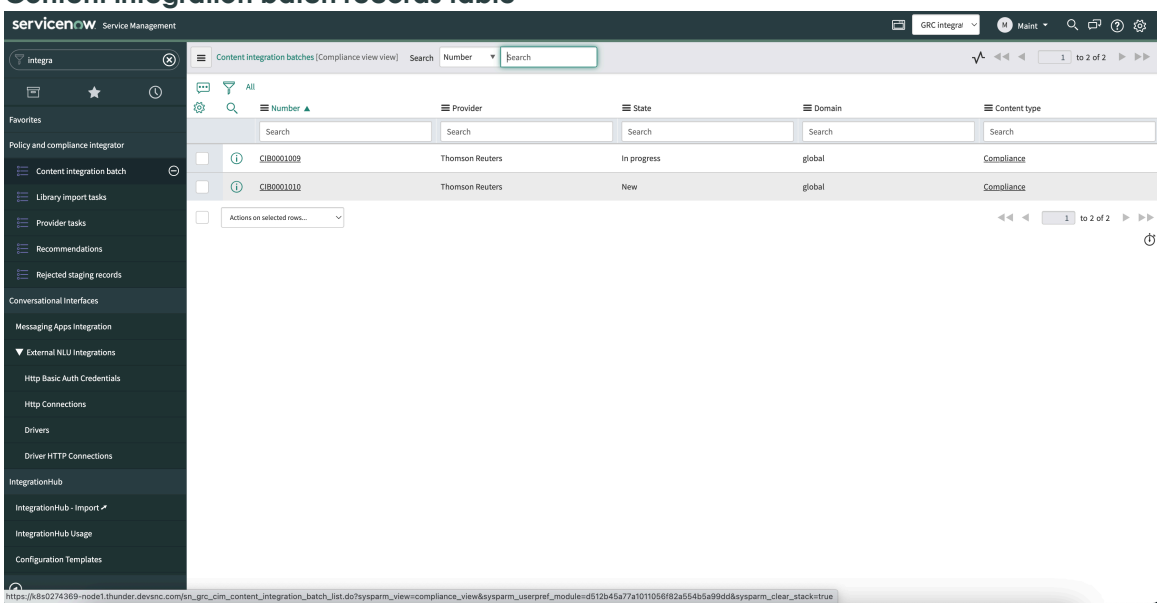
As a user with the sn_compliance.admin role, you can access the batch records in the content integration batch table and create a library import task for each record. The compliance managers assignment group reviews the library import task and imports the staging records into the Policy and Compliance Management tables.

## Details of the content integration batch table

The content integration batch table displays the details that are shown in the following example:

- Number of the content integration batch record. In the example, CIB0001006 is the record number.
- Provider of the content integration batch. In the example, Thomson Reuters is the provider.
- State of the content integration batch. In the example, the state is New.
- Domain of the content integration batch. In the example, the domain is Global.
- Content type of the content integration batch. In the example, the type is Compliance.

### Content integration batch records table



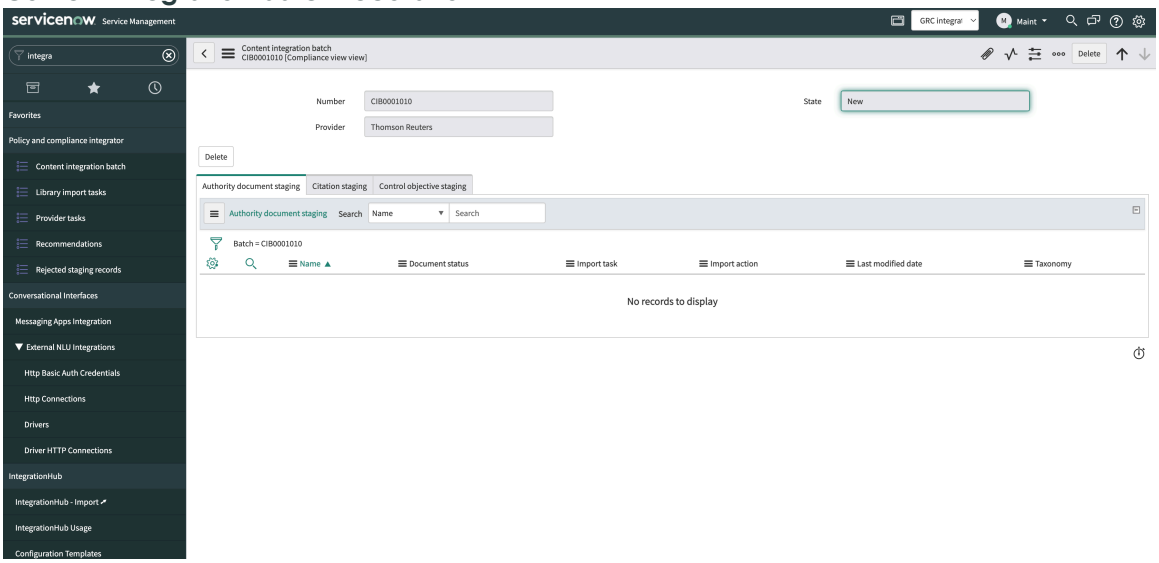

To learn how you can use the user roles to access the APIs and batch records, see User roles for the integration process.

Select a record in the table to display the content integration batch record form and its related lists. See the following example.

**Note:** The fields in the form and the related lists are auto-populated.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

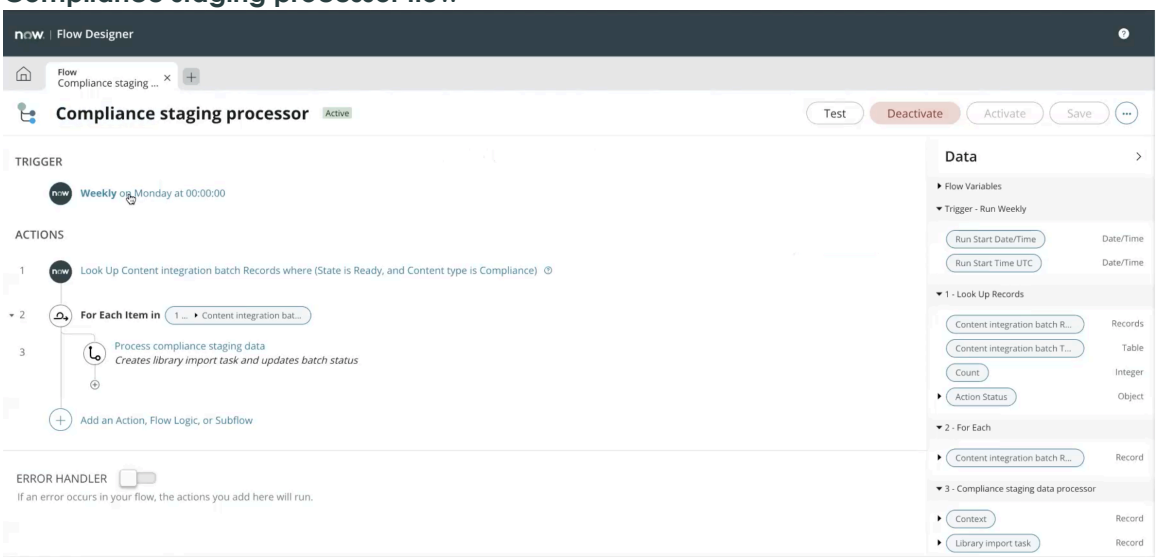
### Content integration batch record form




## Using the Compliance staging processor flow

You can use the new Compliance staging processor flow that is provided with the GRC: Policy and Compliance integrator application. See the following example. The flow is used to process the compliance staging data and it runs in the background on a weekly basis. It searches for the content integration batch records where the state is Ready and the content type is Compliance. For each record in the content integration batch, it creates a library import task and it updates the content integration batch status automatically.

### Compliance staging processor flow




**Note:** You can update the flow to change its setting. For example, you can update the start time of the flow.

## Using the REST APIs

You can use the REST APIs to insert the records in the GRC: integrations with third-party content and later move the records to the Policy and Compliance Management tables by using the GRC: Policy and Compliance integrator application. The following internal APIs are provided with the GRC: integrations with third-party content application and the GRC: Policy and Compliance integrator application:

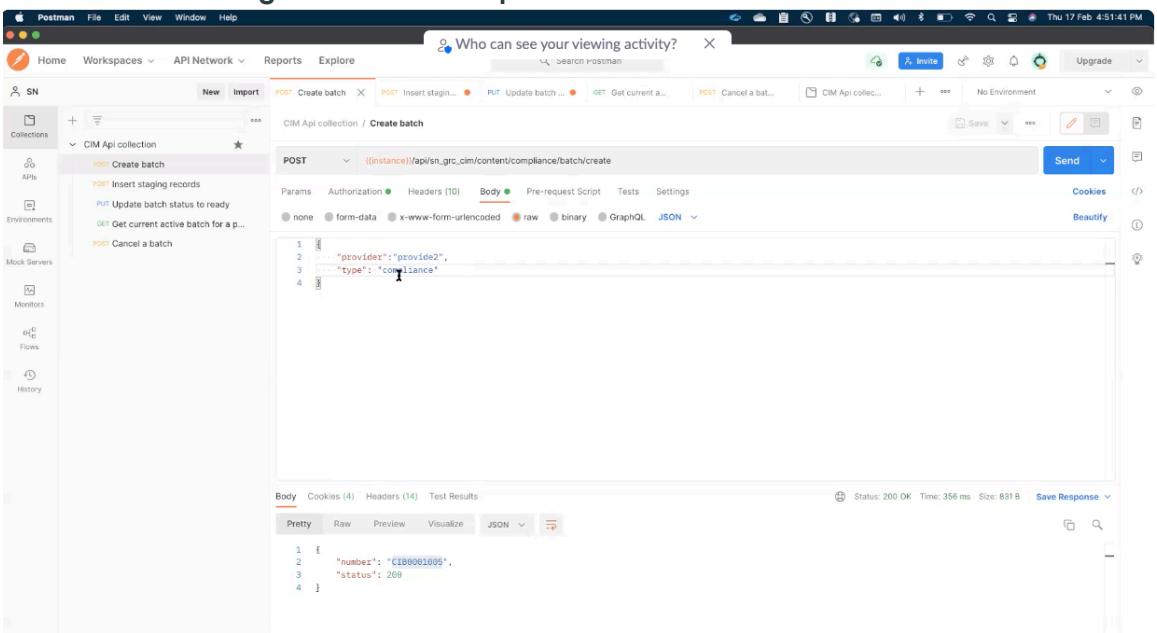
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Create batch
- Insert policy staging records
- Update batch status to ready
- Get batch
- Cancel batch

**Note:** You can use third-party tools, such as the Postman API platform, to execute the APIs.

When you execute the APIs in the Postman API platform as shown in the following example, the staging records are imported in the Policy and Compliance Management tables.

### Create a batch using the Postman API platform



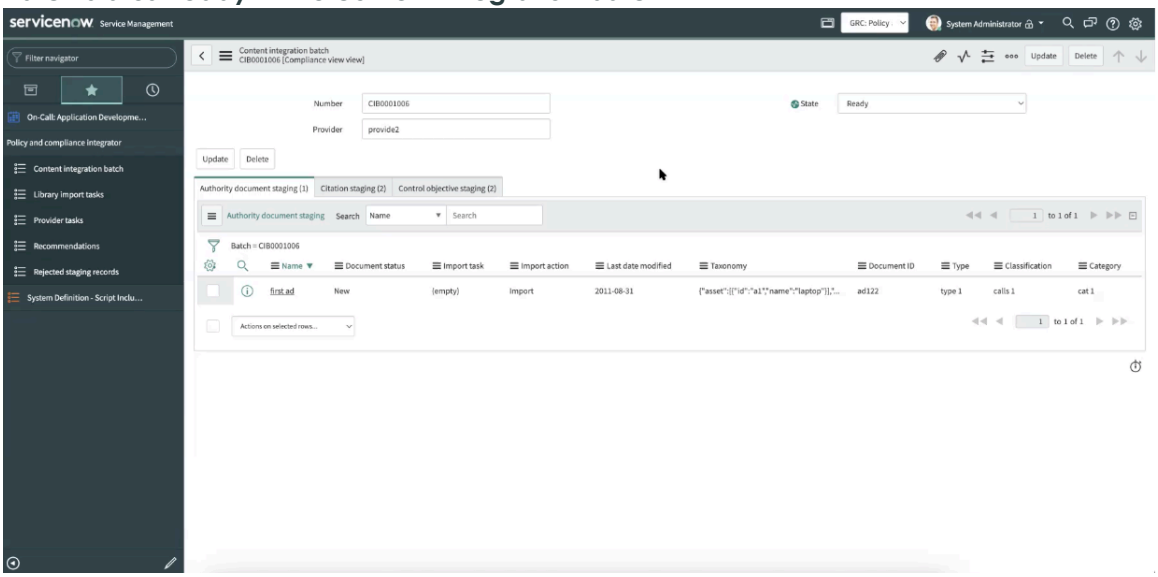

## Processing the batch records

The Update batch status to ready API and the Compliance staging processor flow process the batch records as follows:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. The Update batch status to ready API updates the content integration batch status to Ready as shown in the figure.

**Batch status Ready in the content integration batch**




2. The Compliance staging processor flow picks up the content integration batch and its records. When the Update batch status to Ready API sets the content integration batch status to Ready, the Compliance staging processor flow acknowledges the content integration batch.

3. When the state of the content integration batch is updated to Ready, the Compliance staging processor flow starts importing the records from staging to the GRC: Policy and Compliance integrator application.

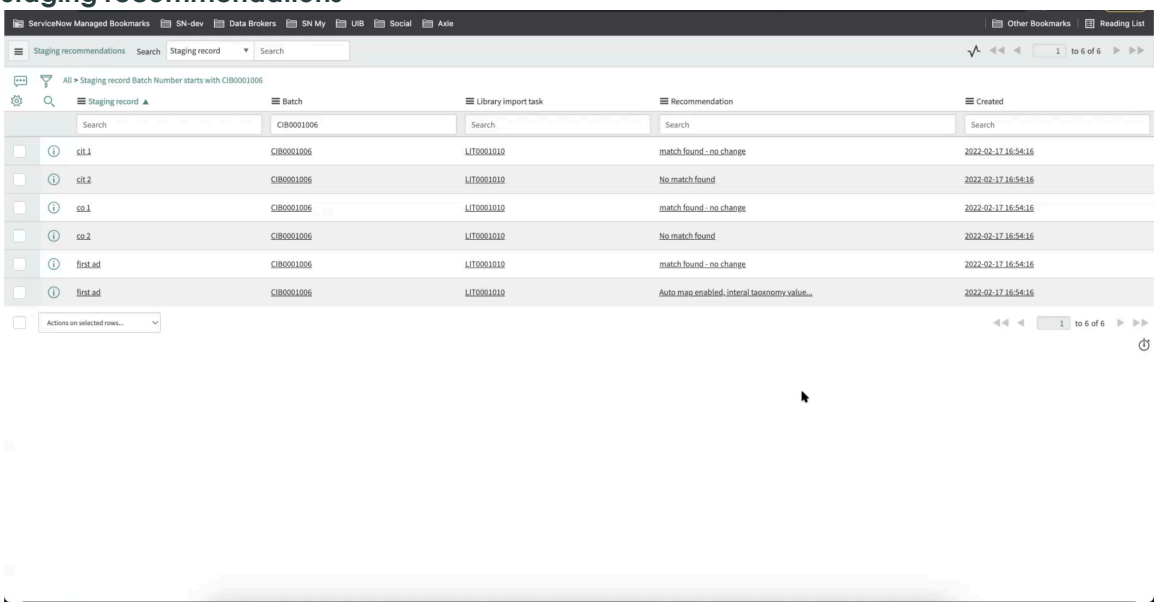
   The system automatically creates a library import task to track the import process.

4. When the library import task is created, the Compliance staging processor flow automatically updates the batch status to In progress.
5. When the library import task is created and the provider that is mentioned in the content integration batch is not found, the state of the task is updated to Provider onboarding. A provider import task is created in the content onboarding task related list of the library import task.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. As the library import task is created, the staging recommendations for each record are generated for the content integration batch as shown in the following example.

**Staging recommendations**




The library import task is used to import the staging records in the Policy and Compliance Management tables. The library import task and staging recommendations for each record are displayed for the content integration batch table in the GRC: Policy and Compliance integrator module. A user with the sn_compliance.admin role can assign the library import task to the compliance managers assignment group. To learn how to assign a library import task, see Assign a library import task for approval.

## Assign a library import task for approval

Assign a library import task to the compliance managers assignment group by using the library import task form in the GRC: Policy and Compliance integrator application.

### Before you begin

For this procedure, you must log in with the sn_compliance.admin role first and then submit the library import task to be approved.

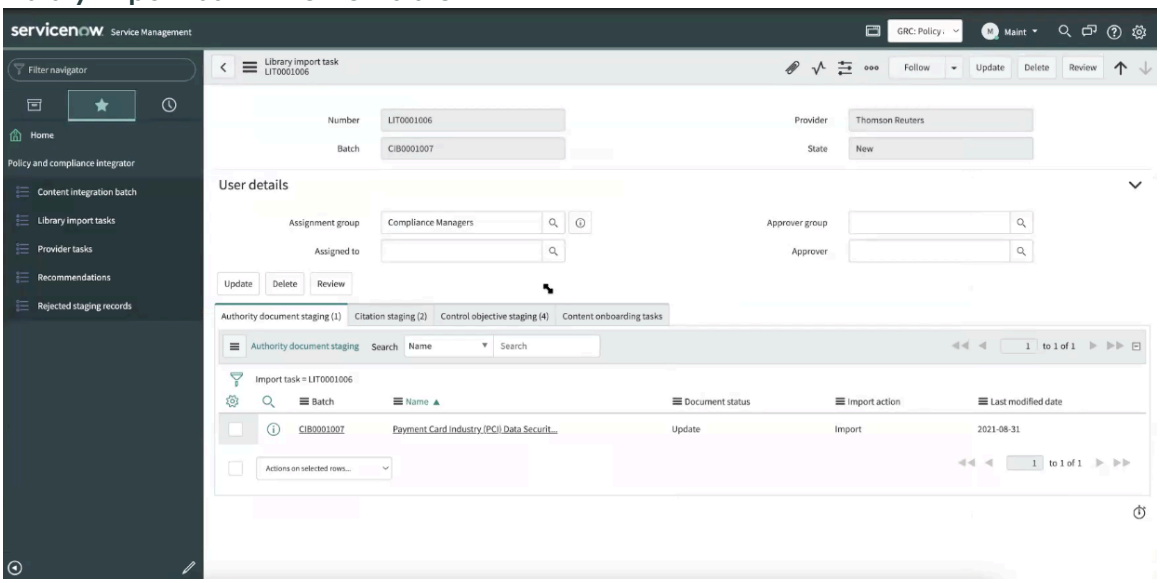
Role required: sn_compliance.admin

### Procedure

1. Navigate to **All** > **Policy and compliance integrator** > **Content integrator** > **Library import task**.
   The library import task is displayed in the New state as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Library import task in the New state




**2.** On the form, fill in the fields.

### Library import task form

| Field | Description |
|---|---|
| Number | Number for the library import task. The number is LIT0001001 in the example. This field is auto-populated. |
| Provider | Name of the provider. This field is auto-populated. |
| Batch | Content integration batch number. The number is CIB0001001 in the example. This field is auto-populated. |
| State | State of the library import task. This field is auto-populated. |
| Assignment group | Assignment group that the library import task is assigned to. Select **Compliance managers** group. |
| Approver | Approver for the library import task. |
| Assigned to | Assignment group that the task is assigned to. |
| Approver group | Approver group for the library import task. |
| Related lists | |
| Authority document staging | Authority document staging records that are related to the library import task. |
| Citation staging | Citation staging records that are related to the library import task. |
| Control objective staging | Control objective staging records that are related to the library import task. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Content onboarding tasks | Provider import tasks that are related to the library import task. This task is created when the provider that is mentioned in the content integration batch is not found in the provider (sn_grc_provider) table.<br><br>If the provider import task is created, the state of the library import task is updated to **Provider onboarding**. When the provider import task is completed, the state of the library import task is updated to **New**. |

3. Click **Update**.

### What to do next

To learn how to approve the library import task that is assigned to the compliance managers assignment group, see Approve the library import task.

## Approve the library import task

Approve the library import task by using the Library import task form in the GRC: Policy and Compliance integrator application.

### Before you begin

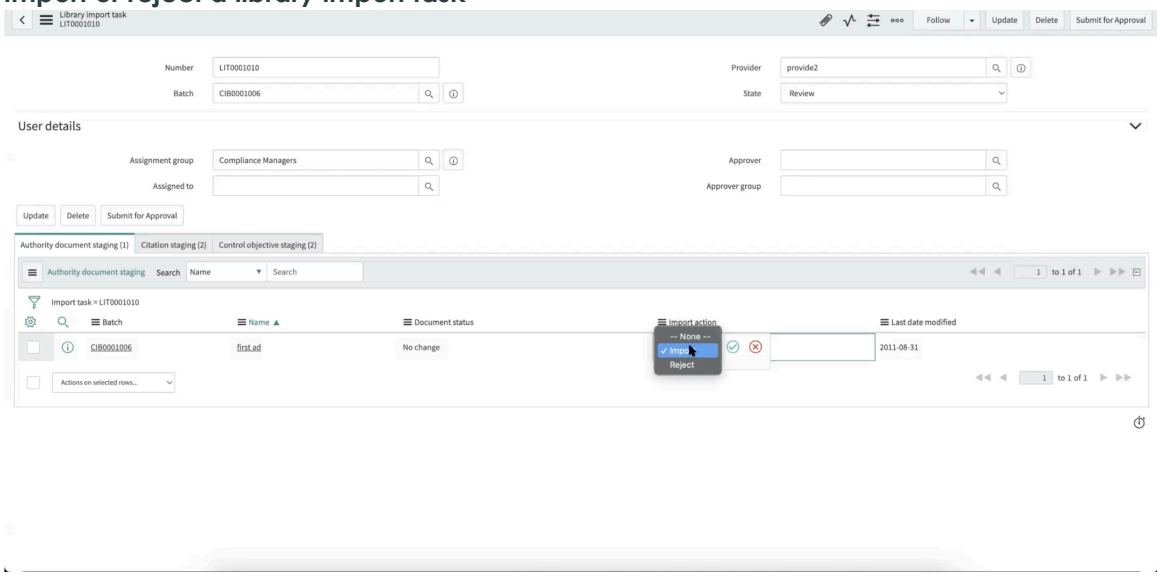
Role required: sn_compliance.manager

### Procedure

1. Navigate to **All** > **Policy and compliance integrator** > **Content integrator** > **Library import task**.
2. Review the library import task and the related lists for the authority document staging records, citation staging records, control objective staging records, and content onboarding tasks.
3. In the application navigator, go to Recommendations and review the recommendations that are provided by the application for the task.
4. On the form, click **Import** or **Reject**.
   Review the details of the library import task and either import or reject the record as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Import or reject a library import task

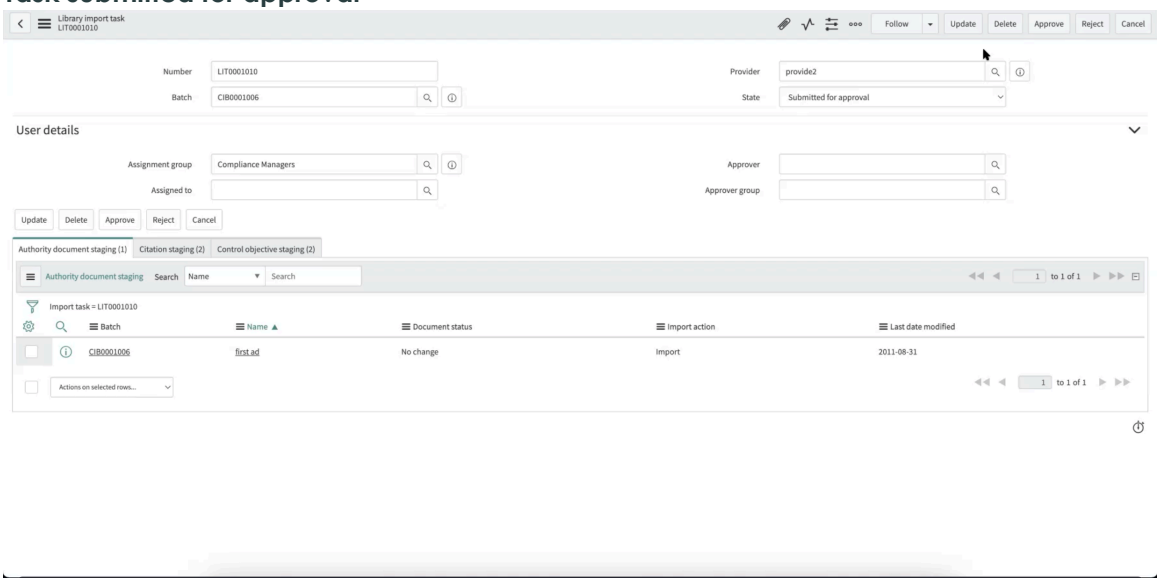



Clicking **Import** imports the record that is associated with the library import task into the GRC: Policy and Compliance Management staging tables.

Clicking **Reject** rejects the record that is associated with the library import task. As a result, the data is not imported into the GRC: Policy and Compliance Management staging tables.

5. Click **Submit for approval**.
   The task is submitted to the compliance managers group for approval. The state of the library import task is updated to Submitted for approval as shown in the following example.

### Task submitted for approval



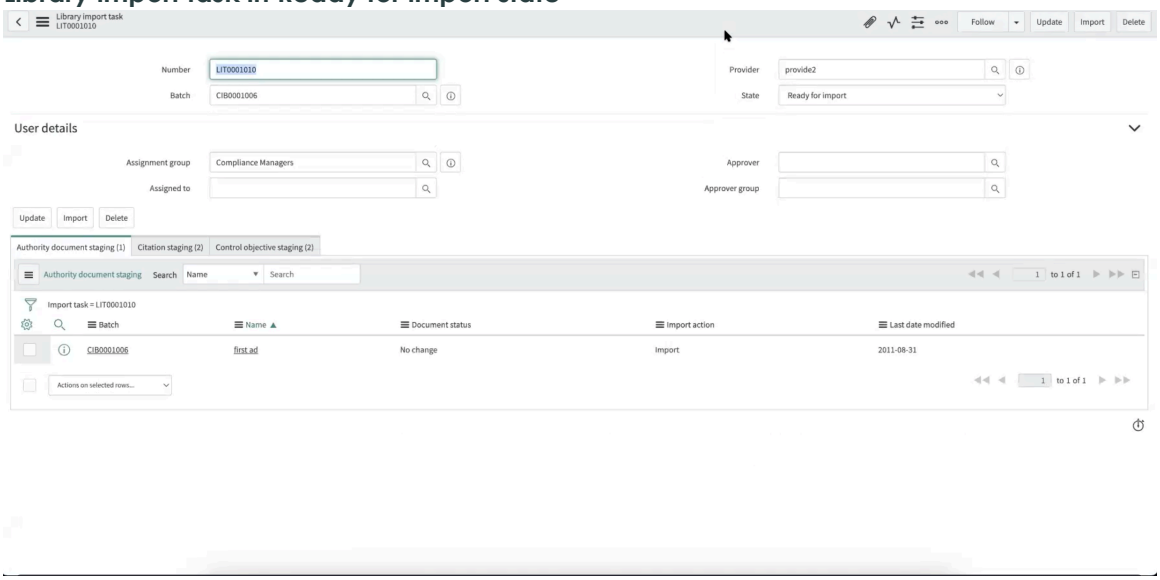

6. Review the library import task and click **Approve**.

   This action moves the library import task to Ready for import state.

   **Note:** Clicking **Reject** rejects the library import task and moves it to New state again as shown in the following example.

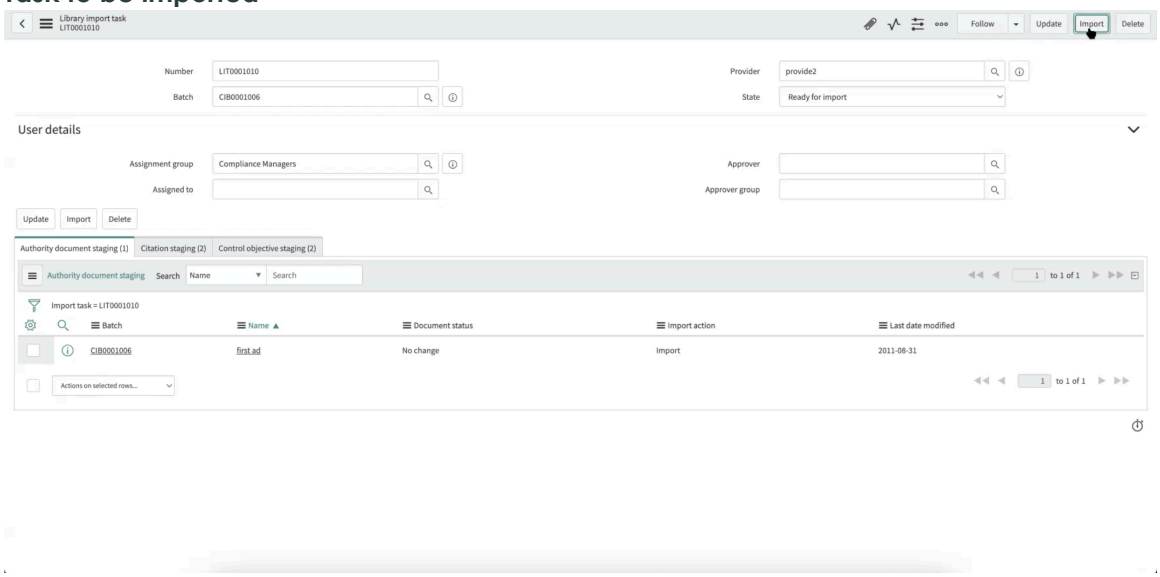
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Library import task in Ready for import state




When the task is in the Ready for import state, the Import action is displayed as shown in the following example.

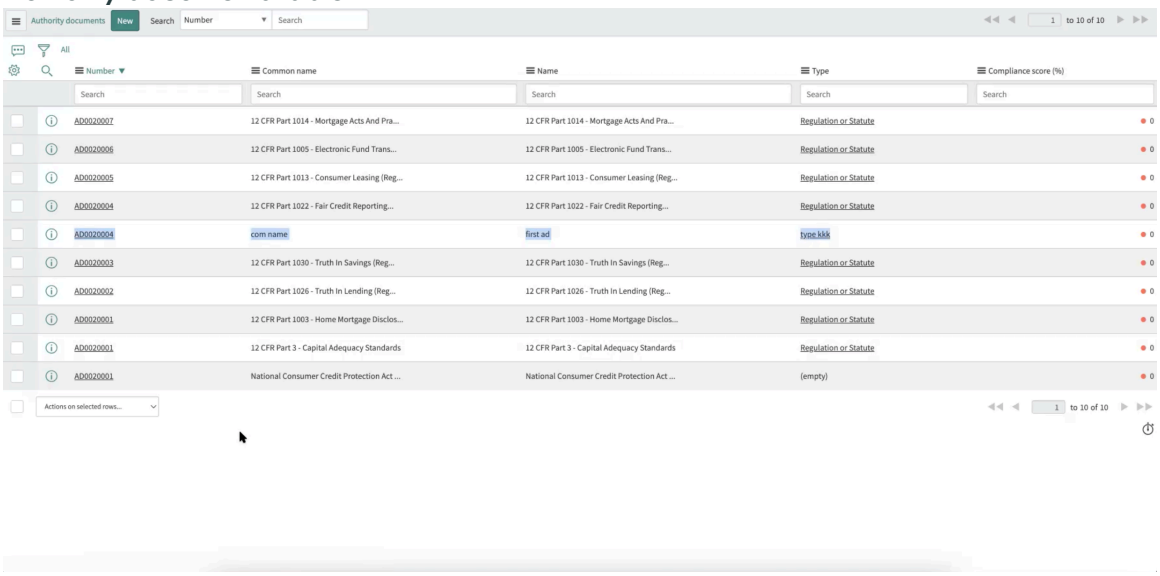
### Task to be imported




7. Click **Import**.
   This action imports the staging records under the library import task into the GRC: Policy and Compliance Management tables. You can view the tables by navigating to the authority document tables, citation tables, or control objectives tables in the GRC: Policy and Compliance Management application. See the sample Authority documents table as shown in the following example.

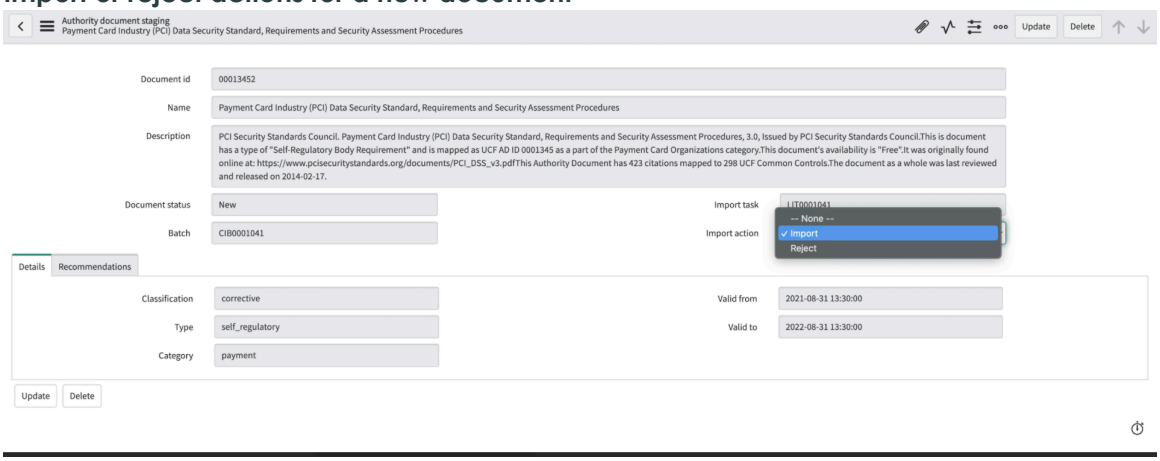
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Authority documents table




When you click an authority document, such as AD0020004 that is displayed in the table, it displays the details of the authority document staging record. In the staging record, the Document status field on the form displays information on the current document status. When the document status field value is New or Update, the Import or Reject actions are available for the record, and the import task can be imported or rejected as shown in the following example.

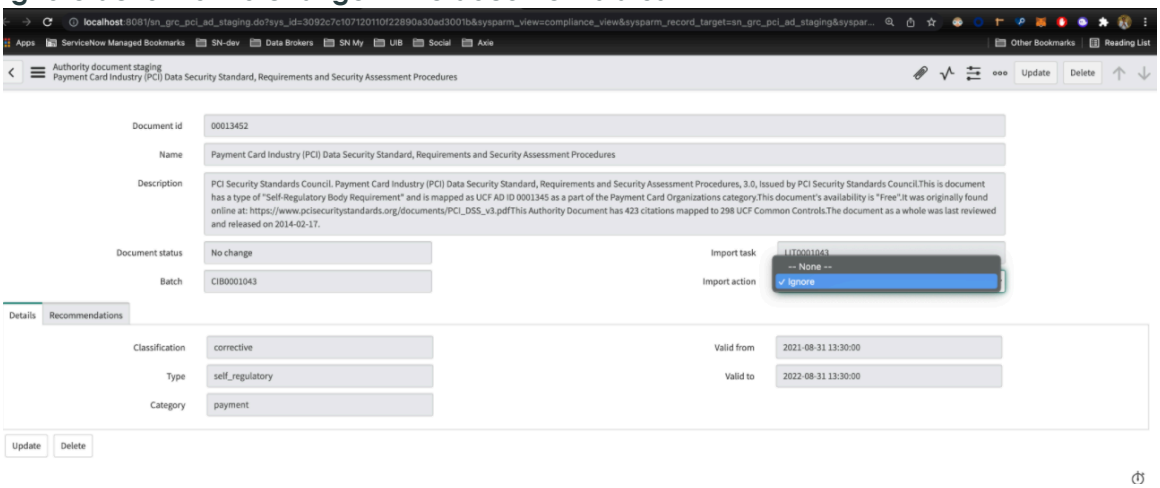
### Import or reject actions for a new document




When the document status field value is No change, only the Ignore option is available in the Import action for the record. The import task can be ignored as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Ignore action for no change in the document status




See the following table for the criteria of the Document status field values.

### Document status field value and its criteria

| Field | Description |
|---|---|
| Document status = New | Record that is not found in the GRC: Policy and Compliance Management tables. |
| Document status = No change | **Source last modified date** of the existing record in the GRC: Policy and Compliance Management table that is later than the incoming staging record date. The document status does not change. |
| Document status = Update | **Source last modified date** of the existing record in the GRC: Policy and Compliance Management table that is earlier than the incoming staging record date. The document status is updated. |

After the workflow is completed, the Compliance staging processor flow automatically updates the status of the library import task to Completed.

**Note:**

If an error occurs in the processing of the flow, the Compliance staging processor flow updates the state of the library import task to Completed with errors. This error can happen due to one of the following reasons:

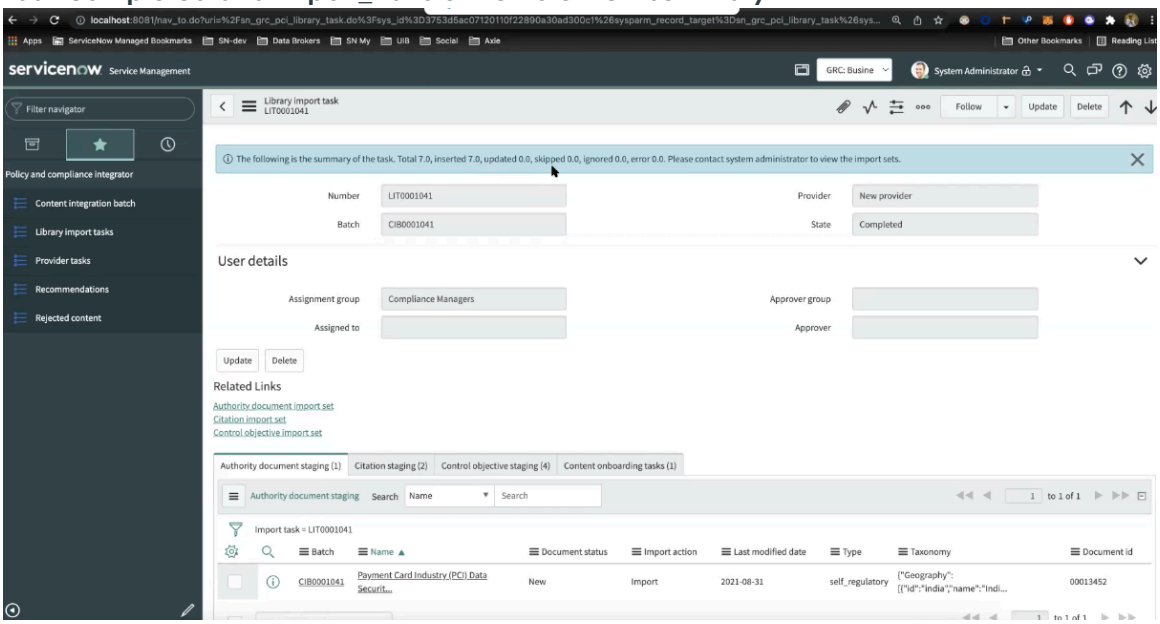
- The taxonomy value mappings of the record are not found and the automap value of the provider taxonomy configuration is false.
- The parent of the record is ignored.

The record with the error is rejected by the Compliance staging processor flow.

When the status of the library import task is Completed, the import task summary and the related links of the import sets are displayed only to the users with the import_transformer role as shown in the following example. The import_transformer role is a global role.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Task completed and import_transformer role view summary**




The import_transformer role view summary is not available to any other users of the GRC: Policy and Compliance integrator application.

**Result**
The library import task is now in the Completed state and the content is imported into the Policy and Compliance Management application.

## Policy as Code Engine for Preventive compliance management

Compliance managers can map the control objective with the Policy as Code Engine (PaCE). PaCE calls GRC passing the document reference and the PaCE policy for which exceptions need to be determined. Control owners can view the PaCE logs to understand the compliance or non-compliance instances.

With increasing number of regulations that organizations must comply with and equally increasing technology risks, organizations are obligated to integrate preventive controls in the digital workflows. For example, when a new software application is developed during a DevOps process, there are several IT policies and controls that have to be implemented and validated to reduce technology risk.

With Policy as Code Engine, you can write your own custom code logic to validate a policy and integrate in a deployable instance. PaCE policy validates the code even before it is committed into a deployable instance and checks for its compliance. If there is non-compliance, the deployment is stopped. To integrate with GRC, PaCE as a policy is added to a control objective using the Compliance Data Source Registry feature.

Preventive compliance management through integration with PaCE prevents compliance team, operations team, DevOps engineers from performing non-compliant activities. On the other hand, this integration helps them to raise exceptions in advance.

Key features of this integration are:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Compliance is embedded in the employee workflows to improve the overall experience of the employees.
- Customers can codify their controls and based on the execution status, employees can be informed if their action in the workflow would determine non-compliance.
- In case of non-compliance, based on a business requirement the employees can request an exception and continue with the digital workflow.

Key benefits through this integration are:

- Reduced reliance on employee training: Since the controls are embedded in the workflows, the number of trainings that employees have to go through are considerably reduced.
- Automated reviews and compliance monitoring: Automated checks ensure that controls are not violated, thereby decreasing the task of manual reviews.
- Automated audit logs: Audit and compliance teams can access the automated audit logs, which reduce the task of manual audits and evidence collection.
- Lower risks and reduced violations: Continuous monitoring of controls minimizes the probability of violations.
- Visibility: Provides real-time visibility of compliance to stakeholders such as business, risk, and compliance teams.
- Velocity: Increases the velocity of workflows as employees can request exceptions if there is business need without impeding the completion of the workflow.

## Configure compliance data source registry

Set up the Compliance Data Source Registry (CDSR) that provides the ability to associate policies in other ServiceNow products with control objectives in Policy and Compliance to inform an organization's overall compliance stand, and to perform policy exceptions when required.

### Before you begin

Role required: sn_compliance.admin

### About this task

Based on the association, entities are generated for the associated assessed objects from the target application table and controls are generated automatically. CDSR facilitates easy integrations between GRC and other ServiceNow products such as DevOps, HR, SecOps, and others to meet the customers' compliance validation and management needs across the enterprise.

Select the application table that is linked to the assessed object table. Establish a relationship between an item in the application table and a control objective in a target table. To do this, the items must first be configured and mapped to the control objective. Secondly, establish a relationship between the target table and the entities in the entity table.

Incidentally, entities are people, processes, departments, applications, or objects that must be measured for compliance against control objectives.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Administration** > **Compliance data source registry**.
2. Click **New**.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Compliance data source registry form

| Field | Description |
|---|---|
| Name | Name of the item registry. |
| Application table | Table of records associated to control objective. |
| Related entity identification | |
| Assessed object table | Table in which controls are created. |
| Relationship to application table | Relationship between the item table and the target table. The choices are:<br>◦ One to many: One record in the application table is linked to multiple records in the assessed object table, and one record in the assessed object table is linked to only one record in the application table.<br>◦ Many to many: One record in the application table is linked to multiple records in the assessed object table, and one record in the assessed object table is linked to multiple records in the application table. |
| Application field on assessed object table | Field name that points to the target table. |
| Application field on m2m table | Field name in the mapping table that points to the item table. |
| Assessed object field on m2m table | Field name in the mapping table that points to the target table. |
| Is the assessed object table equivalent to entities? | Flag to create an entity in the target table. |
| Entity relationship to assessed object table | Relationship between the item table and the entity table. The choices are:<br>◦ One to one: When one record in the assessed object table is linked to only one record in the entity table.<br>◦ Many to many: When one record in the entity table is linked to multiple records in the assessed object table, and when one record in the assessed object table is linked to multiple records in the entity table. |
| Many to many table | Table that establishes the relationship between the item table and the target table. |
| Entity field on assessed object table | Name of the field that points to the entity table. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Entity field on m2m table | Name of the field in the mapping table that points to an entity table. |
| Entity owner field | Owner of the entity in the entity table. |

For more detailed information on the set up of generic framework compliance data source registry, see the Set up of generic framework compliance data source registry [KB1112478] article in the Now Support Knowledge Base.

**Note:** You must log in to Now Support to view the articles.

4. Click **Submit**.

## Associate an item in application table to a control objective

Use the Policy as Code Engine (PaCE) policy related list in the Compliance Workspace to map the control objective with a PaCE policy. Compliance managers have the ability to map the control objectives with PaCE policies.

### Before you begin
Role required: sn_compliance.manager

### About this task
When a PaCE policy is mapped to a deployable instance and if the PaCE policy is already associated to a control objective, then when the association of the policy to the deployable instance occurs a trigger is initiated from Configuration Data Management (CDM) to create an entity and controls.

When a PaCE policy is mapped to a deployable instance, and if the policy is not associated to any control objective, then when the PaCE policy is mapped to the control objective the entity and controls are auto-generated since the deployable instance is already mapped to the policy.

### Procedure
1. Navigate to **All** > **Policy and Compliance** > **Compliance Workspace**.
2. In the Compliance Workspace, click the List icon ( ).
3. Navigate to **Compliance library** > **Control objectives**.
4. Click open a control objective or create a control objective.
5. Click the Details related list.
6. To automatically generate the controls for the control objective, select the **Creates controls automatically** option.
   Whenever an entity type is added to the control objective, controls are automatically generated if the **Creates controls automatically** option is selected.
7. Click **Save** button.
8. To view the controls generated for the control objective, click the Controls related list.
9. Select the **Active** option in the Details related list.

**Note:** The control objective must be active to add a PaCE policy to it. Or, the **Add** and **Remove** buttons in the PaCE policies related list are available only when the control objective is active.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

10. To add the PaCE policy to the control objective, click the PaCE policies related list.
11. Click the **Add** button.
12. Select a PaCE policy from the list of policies that are mapped to the deployable instance in the PaCE policies pop-up.

    **Note:** The PaCE policies that are inactive are listed in the pop-up.

    If the PaCE policy does not have a deployable instance mapped to it at the time of this association, then the entity and the controls are generated whenever the deployable instance is associated to the PaCE policy.

13. Click **Add**.
    The corresponding entities and controls for the configuration items associated to PaCE policy are created if the **Creates controls automatically** option is selected. Existing retired controls are activated if they were not manually retired.

    If an entity has already been added to the control objective as an additional entity, then a control is not created but is updated with a different status. This is to fulfill the condition that only one control can exist per entity. If the control has been generated by the item generation process, then the source of the control is updated. If the control has multiple sources then such control is not retired.

14. To remove a PaCE policy from a deployable instance, click the PaCE policies related list.
15. Click the **Remove** button.
    When the PaCE policy is disassociated from the deployable instance, or when the PaCE policy related to the control objective is removed, then all the entities and controls that were generated earlier from this association are moved to **Retired** state. They are not deleted but continue to exist in retired state.
16. To view the PaCE policy execution results on controls and engagements, click the DevOps Config results related item by navigating to the control record.

## DevOps accelerator for control compliance, PaCE execution, and exception management

GRC: DevOps Accelerator is an application that enables your customers to evaluate the compliance for DevOps policies and GRC control objectives integrating with Policy as a Code Engine (PaCE).

**Important:** Starting with the *Washington DC* release, GRC DevOps Use Case Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances but will continue to be supported.

GRC: DevOps Accelerator (com.sn_grc_devops) plugin maps the control objectives drawn from regulations, standards, and frameworks, such as CIS controls, NIST 800-53, ISO 27002, PCI DSS, and others with DevOps Policy as a Code Engine (PaCE). The DevOps policies are provided by the DevOps Config Policy Content Pack.

With this integration you can evaluate the compliance status. The integration also enables the DevOps managers to monitor control compliance, visualize evidence of PaCE execution, and manage exceptions.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Pre-requisites for DevOps accelerator

1. Hierarchy of PaCE-related plugins and CDM-related plugins.
2. DevOps Config Policy Content Pack provided by PaCE.
3. GRC plugins: GRC: Cybersecurity Controls Accelerator, GRC: Compliance UCF, and GRC: Continuous Authorization and Monitoring.

**Note:** GRC: DevOps Accelerator (com.sn_grc_devops) is dependent on DevOps Config Policy Content Pack and GRC: Policy and Compliance Management. However, if GRC: Cybersecurity Controls Accelerator (CIS), GRC: Unified Compliance Framework (UCF), and GRC: Continuous Authorization and Monitoring (CAM) plugins are not installed on the instance, then the staging data relevant to the control objectives from these plugins would not be available on installing GRC: DevOps Accelerator.

GRC: DevOps Accelerator plugin maps the relationship between PaCE policies and control objectives.

**Note:** Not all GRC control objectives may have a relationship with every PaCE policy.

## Populating control objective and PaCE mapping data from the instances to staging table

Control objective to items mapping table

As part of DevOps accelerator, the mapping relationships between control objectives and PaCE policies are shipped to the customers. The relationship is captured in Control objective to items [sn_compliance_control_objective_item] table, where the **Control objective** column and **Item record** column, which is the PaCE policy, list the data.

### Control objective to item table

Control objective to items | Control objective | Search | Actions on selected rows...

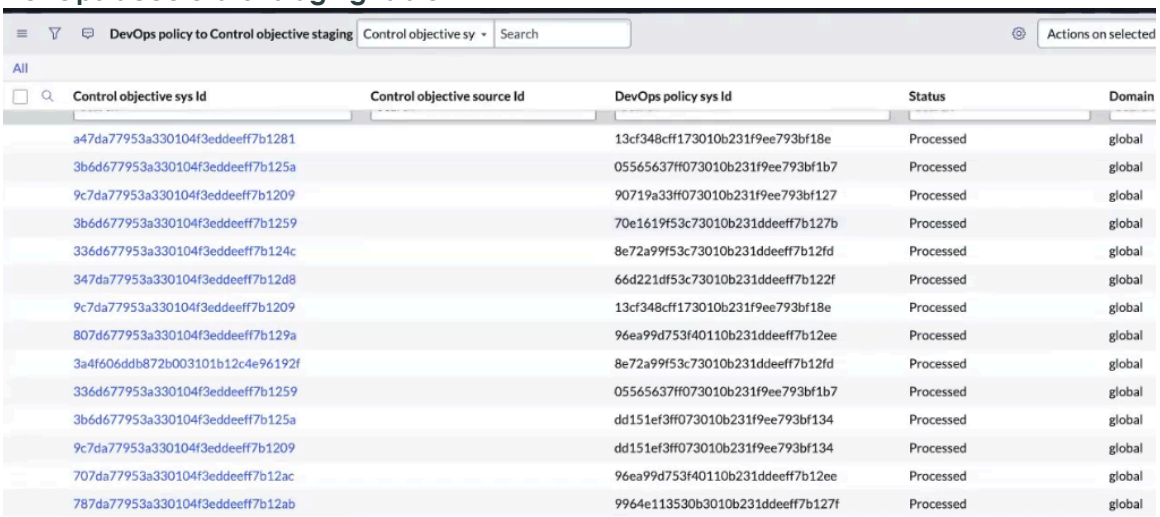
All

| Control objective | Item record | Application table | Assessed object table | Domain |
|---|---|---|---|---|
| Search | Search | Search | Search | Search |
| Encrypt Sensitive Information at Rest | Policy: mandatoryValue | sn_pace_policy | CDM Deployable [sn_cdm_deployable] | global |
| Implement Application Whitelisting of Li... | Policy: forbiddenKVcombinations | sn_pace_policy | CDM Deployable [sn_cdm_deployable] | global |
| Perform Regular Automated Port Scans | Policy: authorisedPortsRange | sn_pace_policy | CDM Deployable [sn_cdm_deployable] | global |
| Encrypt Sensitive Information at Rest | Policy: checkUniqueKeyValue_crossDeployables | sn_pace_policy | CDM Deployable [sn_cdm_deployable] | global |
| Encrypt All Sensitive Information in Tra... | Policy: mandatoryTagsList | sn_pace_policy | CDM Deployable [sn_cdm_deployable] | global |
| Use Multifactor Authentication For All A... | Policy: authorisedKVCombinations | sn_pace_policy | CDM Deployable [sn_cdm_deployable] | global |
| Maintain Standard Security Configuration... | Policy: noHTTP | sn_pace_policy | CDM Deployable [sn_cdm_deployable] | global |
| Establish Secure Coding Practices | Policy: noForbiddenValues | sn_pace_policy | CDM Deployable [sn_cdm_deployable] | global |

DevOps policy to control objective staging table

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### DevOps accelerator staging table




| Control objective sys Id | Control objective source Id | DevOps policy sys Id | Status | Domain |
|---|---|---|---|---|
| a47da77953a330104f3eddeeff7b1281 | | 13cf348cff173010b231f9ee793bf18e | Processed | global |
| 3b6d677953a330104f3eddeeff7b125a | | 05565637ff073010b231f9ee793bf1b7 | Processed | global |
| 9c7da77953a330104f3eddeeff7b1209 | | 90719a33ff073010b231f9ee793bf127 | Processed | global |
| 3b6d677953a330104f3eddeeff7b1259 | | 70e1619f53c73010b231ddeeff7b127b | Processed | global |
| 336d677953a330104f3eddeeff7b124c | | 8e72a99f53c73010b231ddeeff7b12fd | Processed | global |
| 347da77953a330104f3eddeeff7b12d8 | | 66d221df53c73010b231ddeeff7b122f | Processed | global |
| 9c7da77953a330104f3eddeeff7b1209 | | 13cf348cff173010b231f9ee793bf18e | Processed | global |
| 807d677953a330104f3eddeeff7b129a | | 96ea99d753f40110b231ddeeff7b12ee | Processed | global |
| 3a4f606ddb872b003101b12c4e96192f | | 8e72a99f53c73010b231ddeeff7b12fd | Processed | global |
| 336d677953a330104f3eddeeff7b1259 | | 05565637ff073010b231f9ee793bf1b7 | Processed | global |
| 3b6d677953a330104f3eddeeff7b125a | | dd151ef3ff073010b231f9ee793bf134 | Processed | global |
| 9c7da77953a330104f3eddeeff7b1209 | | dd151ef3ff073010b231f9ee793bf134 | Processed | global |
| 707da77953a330104f3eddeeff7b12ac | | 96ea99d753f40110b231ddeeff7b12ee | Processed | global |
| 787da77953a330104f3eddeeff7b12ab | | 9964e113530b3010b231ddeeff7b127f | Processed | global |

There is a staging table as a part of DevOps accelerator, which is DevOps policy to control objective staging [sn_grc_devops_policy_control_objective_staging] table. A user with Compliance admin role can view the table.

For CAM and CIS, the sys IDs of the control objectives map with the DevOps policy sys IDs. However, for UCF the source ID of the control objective imported from the Shared List is mapped with the DevOps policy sys ID.

The data in the DevOps policy to control objective staging [sn_grc_devops_policy_control_objective_staging] table is shipped in Pending status. The data is populated in the staging table based on the applications that are installed in the instance. The data is not processed if the control objective and the PaCE policy do not exist in the instance.

### Scheduled job to move data from the staging to the main table

A daily job (Import DevOps policy to Control Objective mapping from staging) runs after the applications and the DevOps accelerator are installed to add the records to the Control objective to items (sn_compliance_control_objective_item) table. If the record is successfully added to the mapping table, then the status of the record in the staging table moves to Processed. If a control objective is not populated or present in the application, then the record is not processed but is in Pending status.

## Manage continuous monitoring for controls between Configuration Compliance and Policy and Compliance Management

Continuous monitoring for controls is a feature integration between the GRC: Policy and Compliance Management product and the Security Operations Configuration Compliance products. This feature integrates the scan results from third-party applications, like Qualys to determine the compliance status for each associated control.

Continuous monitoring is a pro-active security management approach. Customers monitor and validate compliance and manage risks against authority documents.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Continuous monitoring workflow

1. The system admin activates the Configuration Compliance and Policy and Compliance Management plugins.
2. The compliance manager maps control objectives or controls to configuration tests, which generate controls, entities, and indicators related to those configuration tests.
3. The integration ingests the results of the third-party configuration test scan results at defined intervals.
4. If the configuration test scan results of the configuration tests indicate a failure, then the control is non-compliant and an issue is automatically generated.
5. If the next scan result of the configuration test indicates that the failure has been remediated, then the control is compliant and the issue is automatically closed.

## Map control objective or controls to configuration tests

The compliance manager maps control objectives or controls to the configuration tests, which generate the controls, entities, and indicators associated with configuration compliance.

### Before you begin

Role required: compliance manager

The Configuration Compliance plugin must be activated to access this feature and the **sn_compliance.auto_create_profile_and_control** property must be set to true.

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Policies**.
2. Open the policy record, click the Control Objectives related list, and click **Edit**.

   **Note:** The **Password** Policy is used in this example.

3. Select each control objective to associate to the policy.
4. Open a control objective, and click the Citations related list to view the authority document citation that is associated to this control objective.

   **Note:** The **Configure the maximum password age** control objective is used in this example.

5. Click the Configuration Tests related list and select one of the following add options:
   - Click **Add**
   - Click **Add from Policies**
   - Click **Add from Authoritative Sources**

   **Note:** The **Source** field for each configuration test identifies the third-party provider of the information.

6. After selection, click **Add**.
   All the configuration items (controls, entities, and indicators) are mapped and displayed on the Configuration Tests related list. The results may take a few minutes to generate.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Interpret configuration compliance scan results

If the configuration test scan results of the control indicate any failures, the control is marked non-compliant. If the scan results indicate the control passed, all the configuration tests, then the control is marked compliant.

#### Before you begin

Role required: compliance manager

The Configuration Compliance plugin must be activated to access this feature and the *sn_compliance.auto_create_profile_and_control* property must be set to true

#### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Policies and Procedures** > **Control Objectives**.

   **Note:** The **Configure the maximum password age** policy statement is used in this example.

2. Open the control objective record and click the Controls related list.
   11 controls were generated from the configuration compliance test scan. Each control has an associated **Profile** and because all the controls show a **Status** of **Non Compliant**, an equal number of issues have been automatically generated.
3. Open a control record, and click the Indicator related list.
4. Open the indicator record to see the indicator results.
   The configuration test scan results are updated at regular intervals. If the scan results indicate that the failure has been remediated, then the control is marked compliant and the issue is automatically closed.

## Policy and Compliance Management reference

Reference topics provide information about tables, roles, and properties installed with the GRC: Policy and Compliance Management application.

### Components installed with Policy and Compliance Management

Reference topics provide additional information about components that are installed with the activation of the Policy and Compliance Management plugin. These components include tables, user roles, and properties.

**Note:** The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

#### Tables installed with Policy and Compliance Management

Tables are added with activation of GRC: Policy and Compliance Management.

**Tables installed**

| Table | Description |
|---|---|
| Authority Document<br><br>[sn_compliance_authority_document] | Extends the Document [sn_grc_document] table and stores all Authority Documents. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tables installed (continued)**

| Table | Description |
|---|---|
| Control<br><br>[sn_compliance_control] | Extends the Item [sn_grc_item] table and stores all controls. |
| Policy<br><br>[sn_compliance_policy] | Extends the Document [sn_grc_document] table and stores all policies. |
| Article Template<br><br>[sn_compliance_article_template] | Used to format the policy text contained in a policy record when publishing the policy to the knowledge base (KB). |
| Citation<br><br>[sn_compliance_citation] | Extends the Content [sn_grc_content] table and stores all citations. |
| Policy exception risk rating mapping [sn_compliance_policy_exception_risk_rating_mapping] | Stores the mapping details of the risk assessment rating with the policy exception risk rating. |
| Policy to Entity Type<br><br>[sn_compliance_m2m_policy_profile_type] | Extends Document to Entity Type [sn_grc_m2m_document_profile_type] and is a many-to-many relationship table that is used to manage the relationships between policies and entity types. |
| Control Objective to Citation<br><br>[sn_compliance_m2m_statement_citation] | Many-to-many relationship table is used to manage relationships between control objectives and their related citations. |
| Control Objective to Entity Type<br><br>[sn_compliance_m2m_statement_profile_type] | Extends Content to Entity Type [sn_grc_m2m_content_profile_type] and is a many-to-many relationship table that is used to manage the relationships between control objectives and entity type. |
| Control objective<br><br>[sn_compliance_policy_statement] | Extends the Content [sn_grc_content] table and stores all control objectives. |
| Control objective requirement<br><br>[sn_compliance_policy_stmt_requirement] | Stores the requirement number and the requirement description of a control objective requirement. |
| Control objective to Control objective requirement<br><br>[sn_compliance_m2m_policy_stmt_policy_stmt_rqmt] | Many-to-many relationship table is used to manage relationships between control objective and control objective requirement. |
| Control requirement<br><br>[sn_compliance_control_requirement] | Stores the requirement number of control |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tables installed (continued)**

| Table | Description |
|---|---|
| Control to Control requirement<br><br>[sn_compliance_m2m_control_control_requirement] | Many-to-many relationship table that stores the control and control requirement details. The **Implementation status** field gives the information whether the requirement is inherited or self-implemented. |
| Requirement selection<br><br>[sn_compliance_hybrid_selection] | Stores the selections of control requirements. It contains the details of control requirements, control objective, entity, and authorization package. |
| Policy exception<br><br>[sn_compliance_policy_exception] | Stores all policy exceptions. |
| Policy to Policy Statement<br><br>[sn_compliance_m2m_policy_policy_statement] | Many-to-many relationship table is used to manage relationships between policy and control objectives. |
| Control to entity [sn_compliance_m2m_control_entity] | Extends Item to entity [sn_grc_m2m_entity_item] table. |

**Note:** All additional tables installed by the dependent plugins are also needed for Policy and Compliance Management.

### Roles installed with GRC: Policy and Compliance Management

Roles are added with activation of GRC: Policy and Compliance Management.

**Roles installed**

| Role title [name] | Description | Contains roles |
|---|---|---|
| Compliance Administrator<br><br>[sn_compliance.admin] | Contains the reader, user, manager, and admin roles in sn_grc scopes, and the reader, user, and manager roles in the Policy and Compliance Management application. In addition to the inherited permissions, the compliance admin can delete authority documents, citations, policies, control objectives, and controls. | • sn_compliance.manager<br>• sn_grc.admin |
| Attestation Creator<br><br>sn_compliance.attestation_creator | Role used for creating the GRC attestation metric type, as well as exception questionnaires. | assessment_admin |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| Compliance Developer<br><br>[sn_compliance.developer] | Contains the reader, user, manager, admin, and developer roles in sn_grc scopes, and the reader, user, manager, and admin roles in the Policy and Compliance Management application. In addition to the inherited permissions, the compliance developer can create article templates and edit scripts. | • sn_compliance.admin<br>• sn_grc.developer |
| Compliance Manager<br><br>[sn_compliance.manager] | Contains the reader, user, and manager roles in sn_grc scopes, and the reader and user roles in the Policy and Compliance Management application. In addition to the inherited permissions, the compliance manager can create authority documents, citations, control objectives, and controls. | • sn_compliance.user<br>• sn_grc.manager<br>• sn_vdr_risk_asmt.vendor_assessment_review |
| Compliance Reader<br><br>[sn_compliance.reader] | Contains the reader role in sn_grc scopes. In addition to the inherited permissions, the compliance reader can be assigned indicators templates, indicators, and issues. | • sn_grc.reader<br>• survey_reader |
| Compliance User<br><br>[sn_compliance.user] | Contains the reader and user roles in sn_grc scopes, and the reader role in the Policy and Compliance Management application. In addition to the inherited permissions, the compliance user can be assigned controls and create policies, and has read-only access to the Risk Management application and modules. The compliance user can also create control objectives. | • sn_compliance.reader<br>• sn_grc.user<br>• sn_risk.reader<br>• survey_reader<br>• vendor_reader |
| Corporate compliance analyst<br>[sn_compliance_ws.corporate_compliance_analyst] | Contains the reader and user roles in sn_grc scopes, and the reader role in the Compliance Workspace. | • sn_compliance.user<br>• sn_audit.user |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| Corporate compliance manager [sn_compliance_ws.corporate_compliance_manager] | Contains the reader, user, and manager roles in sn_grc scopes, and the reader and user roles in the Compliance Workspace. | • sn_compliance.manager<br>• sn_compliance_ws.corporate_compliance_reader<br>• sn_audit.manager |
| IT compliance manager [sn_compliance_ws.it_compliance_manager] | Contains the reader, user, and manager roles in sn_grc scopes, and the reader and user roles in the Compliance Workspace. | • sn_compliance.manager<br>• sn_audit.manager |

### GRC business user role to control access of compliance tables

The access control limitations (ACLs) or no role conditions with snc_internal role (or no role) is replaced with sn_grc.business_user role to control the access level of different users to compliance tables and also to track their usage.

GRC business user (sn_grc.business_user) role

GRC business user role is granted to users who could perform any GRC operations. It is also granted to users with snc_internal role who have performed all operations like creating policy exception, issues, and responding to attestations, acknowledgements, and other operations. This role comes with installing GRC Profiles plugin.

GRC business user – lite (sn_grc.business_user_lite) role

Users who could do limited operations with snc_internal role are considered as lite operators. Such users are given the GRC business user – lite (sn_grc.business_user_lite) role so as to track the lite usage of compliance tables using the role. This role is granted through explicit roles plugin, GRC: Business User – Lite, which can be installed by users with maint access or ServiceNow support teams.

For more information on install, upgrade, and role assignments, see GRC Business User Role [KB0864247] article in the Now Support Knowledge Base.

**Note:** You must log in to Now Support to view the articles.

The access limitations of users with GRC business user role and other roles for different compliance tables and other related tables are listed herewith. For more information, see the Security tightenings for GRC: Policy and Compliance Management [KB1112315] article in the Now Support Knowledge Base.

Control Objective

- Users with GRC business user or business user lite role can read all control objectives.
- If GRC: Audit Management application is installed and the control objective has a published policy associated to it, then users with external auditor role can read such control objectives.
- Users with business user lite have read access to report an issue or policy exception.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Policy

- Users with GRC business user or business user lite role can read all policies.
- If GRC: Audit Management application is installed, users with external auditor role can read all published policies.
- Users with business user lite have read access to policies so as to create policy exceptions.

Policy to Control Objective M2M

- Users with GRC business user or business user lite role can read a policy to control objective M2M record.
- If GRC: Audit Management application is installed, users with external auditor role can read a policy to control objective M2M record if the policy is published.

Control [sn_compliance_control]

- Users with GRC business user or business user lite role can view a control.
- If GRC: Audit Management application is installed, users with external auditor role can read a control.

Assessment Instance [asmt_assessment_instance]

- Users with GRC business user and business user lite role can view attestations that are assigned to them.
- ServiceNow users with GRC business user or business user lite role can take assessments.
- Users with GRC business user or business user lite role can view My Grouped Attestations module.
- Users with GRC business user and business user lite role can view Group Assessment UI and Ungroup Assessment UI actions.
- Users with GRC business user and business user lite role can view **My Attestations** option in GRC application menu.

Assessment Metric Type [asmt_metric_type]

User role is set to GRC business user or business user lite if the evaluation is attestation, the table is Policy Exception, and the role is empty.

Control Overview report

User with GRC reader role can view the control overview report.

Issue [sn_grc_issue]

Report and View issues in Service Portal

Users with GRC business user or business user lite role can report an issue and view their reported issues in Service Portal. GRC business user or business user lite role is the minimum role required to view **My Issues** in Service Portal.

Read

Users with the following roles can view an issue:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- GRC user (sn_grc.user) role
- GRC business user or business user lite role. Furthermore, the user must fulfil any one of the following conditions:
  - **Assigned to** field in the issue is the user.
  - **Assigned to** of the parent issue is the user or **Assignment group** of the parent issue is one of the user's groups.
  - **Assignment group** is one of the user's groups. Additionally, the user must also have the GRC business user role.
  - **Issue manager** is the user.
  - **Issue manager group** is one of the groups that belong to the logged in user.
  - **Control/Risk** of the issue has an owner and the owner is the user.
  - Issue is created by the logged in user.
  - Issue is created out of an issue triage opened by the user.
  - Logged in user is the assignee or watchlist user on a remediation task for the issue.
  - If GRC: Audit Management is installed, you are an external auditor only; and an auditor on a closed engagement that had control test issues or other issues, can view only those issues.

Write

If the user with the business user role is also the user designated in the **Assigned to** field, then the user can edit:

- Name
- Description
- Issue manager
- Issue manager group
- Action plan
- State
- Parent issue
- Additional comments
- Work notes
- Response
- Explanation

If the user with the business user lite role is also the user designated in the **Assigned to** field, then the user can edit:

- Issue manager
- Issue manager group
- State
- Parent issue
- Additional comments

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Work notes
- Response
- Explanation

**Note:** However, a GRC user can edit all issues.

View My Open Issues

Users with a minimum role of a GRC business user or business user lite can view their open issues.

Issue grouping

Issue grouping is only open to users with GRC user role.

Send information

A minimum of GRC business user or business user lite role is required to send information for the issue.

Issue Source [sn_grc_issue_source]

A minimum of GRC business user role is required to view and edit the Issue Source table.

Remediation task [sn_grc_task]

- User in the **Assigned to** field of the Remediation task table must have a minimum of GRC business user or business user lite role.
- For read access, users who have a remediation task assigned to them or who are the watchlist users on the remediation task must have a GRC business user or business user lite role. The **Assigned to** user of the issue, the issue manager of the issue, or any user with GRC manager (sn_grc.manager) role can view a remediation task.
- **My Open Remediation Tasks** is visible to users with a minimum role of GRC business user or business user lite.

My Indicator Task [sn_grc_indicator_task]

Users with GRC business user role can access My Indicator Tasks.

Policy Acknowledgement

Users with GRC business user or business user lite role can:

- Acknowledge policies from Now Platform UI and Service Portal.
- View **My Acknowledgements** menu option in Service Portal.
- View Acknowledgement instances [sn_compliance_policy_acknowledgement_instance] that are assigned to them.

Policy Exception [sn_compliance_policy_exception]

Users with GRC business user or business user lite role can:

- Raise Policy Exceptions from Now Platform and Service Portal.
- View policy exception. Users with read access include users who requested policy exception, are present in watch list, and are verification approvers, final approvers, impacted control owners, and compliance managers.

For more information, see:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- GRC Business user role [KB0864247] article in the Now Support Knowledge Base.
- Governance, Risk, and Compliance License Compliance update [KB1096178] article in the Now Support Knowledge Base.

### Properties installed with GRC: Policy and Compliance Management

Properties are added with activation of GRC: Policy and Compliance Management.

| Name | Description |
|---|---|
| States for which the control is active (the first state is the default active state)<br><br>sn_compliance.active_states | Compliance administrators can change this setting.<br>• **Type**: string<br>• **Default value**: draft, assess, review, monitor<br>• **Location**: **Policy and Compliance** > **Administration** > **Properties** |
| States for which control is inactive (the first state is the default inactive)<br><br>sn_compliance.closed_states | Compliance administrators can change this setting.<br>• **Type**: string<br>• **Default value**: retired<br>• **Location**: **Policy and Compliance** > **Administration** > **Properties** |
| Name of the assessment metric type that is used for attestations<br><br>sn_compliance.default_attestation | System administrators can change this setting.<br>• **Type**: string<br>• **Default value**: GRC Attestation<br>• **Location**: **Policy and Compliance** > **Administration** > **Properties** |
| sn_compliance.glide.script.block.client.globals | • **Type**: true or false<br>• **Default value**: false<br>• **Location**: **Policy and Compliance** > **Administration** > **Properties** |
| Name of the knowledge base used to publish Policy articles<br><br>sn_compliance.knowledge_base | Compliance administrators can change this setting.<br>• **Type**: string<br>• **Default value**: Governance, Risk, and Compliance<br>• **Location**: **Policy and Compliance** > **Administration** > **Properties** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Domain separation in GRC: Policy and Compliance Management

Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

### Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

For more information on support levels, see Application support for domain separation.

### Overview

Domain separation is best for those customers who:

- Need to enforce absolute data segregation between business entities (data separation).
- Customize business process definitions and user interfaces for each domain (delegated administration).
- Maintain some global processes and global reporting in a single instance.

These users can choose to expand or collapse the domain scope to show or hide data from other domains.

**Note:** Users always have access to data from domains that have been explicitly granted to them by domain visibility.

### How GRC handles domain separation

While GRC supports separation of data, separation of logic and process is not fully supported.

- Many types of records in GRC are automatically generated through user processes. Entities, controls, risks, indicators, and control tests are all records that can be generated automatically. For records that are automatically generated (and for any GRC record that is manually generated), the domain of the record is the same as the domain of the user responsible for creating or generating the records.
- Automatic generation should be kept in mind when working in a domain-separated GRC implementation. Users should be sure that they are creating / generating records at the right domain level so that they are visible to the right set of users.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For example, suppose you have domains that look like:

**Domain separation**




- If you have a risk or control that you want to be assessed by users in domains A and B, the risk or control should be generated or manually created at the global level. If the risk or control is created in Domain B, you will not be able to recreate the risk or control in Domain A due to indexing.
- If you have a risk or control that you want to be assessed by users in TOP and Domain A, you can create the risk or control in Domain A.

Unless the risks and controls are in the Global domain, users should not assign risks or controls in a higher domain to users in a lower domain. In the example above, if you have a control in the TOP domain, you should not assign it for attestation to users in Domains A or B since those users would not have access to the control; thus the attestation or assessment questionnaire would not be generated.

Similarly, users should not assign control objectives and risk statements in a higher domain to attestations and assessments in a lower domain. Otherwise the attestation or assessment questionnaire would not be generated.

## Use case

GRC data for IT can be separated from the GRC data of other departments. Each business area using the GRC application can have separate data that cannot be shared with other departments. Therefore each department can have its own entities, policies, controls, risks, and so on.

When looking at a control from the IT domain, the user can choose to expand the domain scope to show values from the Finance domain or collapse the domain scope to show only controls that match the IT domain.

By default, domain separation adds a domain field to the Task `[task]` and Configuration Items `[cmdb_ci]` tables and their extensions.

You can extend domain separation to any new tables you create by adding a `sys_domain` field to the table's dictionary definition. By default, the system only domain-separates platform and baseline application tables where appropriate.

**Warning:** ServiceNow does not recommend domain separating platform tables (any table with the sys_ prefix such as the Dictionary Entry `[sys_dictionary]` and Dictionary Entry Override `[sys_dictionary_override]` tables) because it can produce unexpected results.

In this use case, client scripts, business rules, workflows, processes, and so on can be domain-separated.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

While the behavior offered with domain separation provides multi-tenancy support, multi-tenancy is still contained within a single instance. This means that some global properties, some global data, and some global processes are shared across all domains. For example, the system's "Remember me" option on the login page is global and cannot be specified per domain.

If you need complete and total separation of all system properties and do not require global reporting or global processes, separate instances are the best option.

Related topics

Domain separation for service providers

## Analytics and Reporting solutions for GRC: Policy and Compliance Management

Analytics and Reporting Solutions contain preconfigured dashboards. These dashboards contain actionable data visualizations that help you improve your business processes and practices.

The Analytics and Reporting Solution for GRC: Policy and Compliance Management is available on the ServiceNow Store.

### Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Use the Platform Analytics widgets on the dashboard to visualize data over time, analyze your business processes, and identify areas of improvement. With Platform Analytics Solutions, you can get value from Performance Analytics for your application with minimal setup. You can always create your own objects as well.

**Important:** Set up and test Platform Analytics Solutions on a non-production instance before enabling them in production.

To enable the Analytics and Reporting solution for GRC: Policy and Compliance Management, perform these steps.

1. Visit the ServiceNow Store and obtain an entitlement to the Performance Analytics - GRC: Policy and Compliance Management application and associated applications. See Install a ServiceNow Product on the ServiceNow Store.
2. On the instance, navigate to **System Applications** > **All Applications** > **All**.
3. Locate and install the Performance Analytics - GRC: Policy and Compliance Management application.

### GRC Compliance Overview dashboard

The Compliance Overview dashboard provides an executive view into compliance requirements, overall compliance, and compliance breakdowns so areas of concern can be identified quickly.

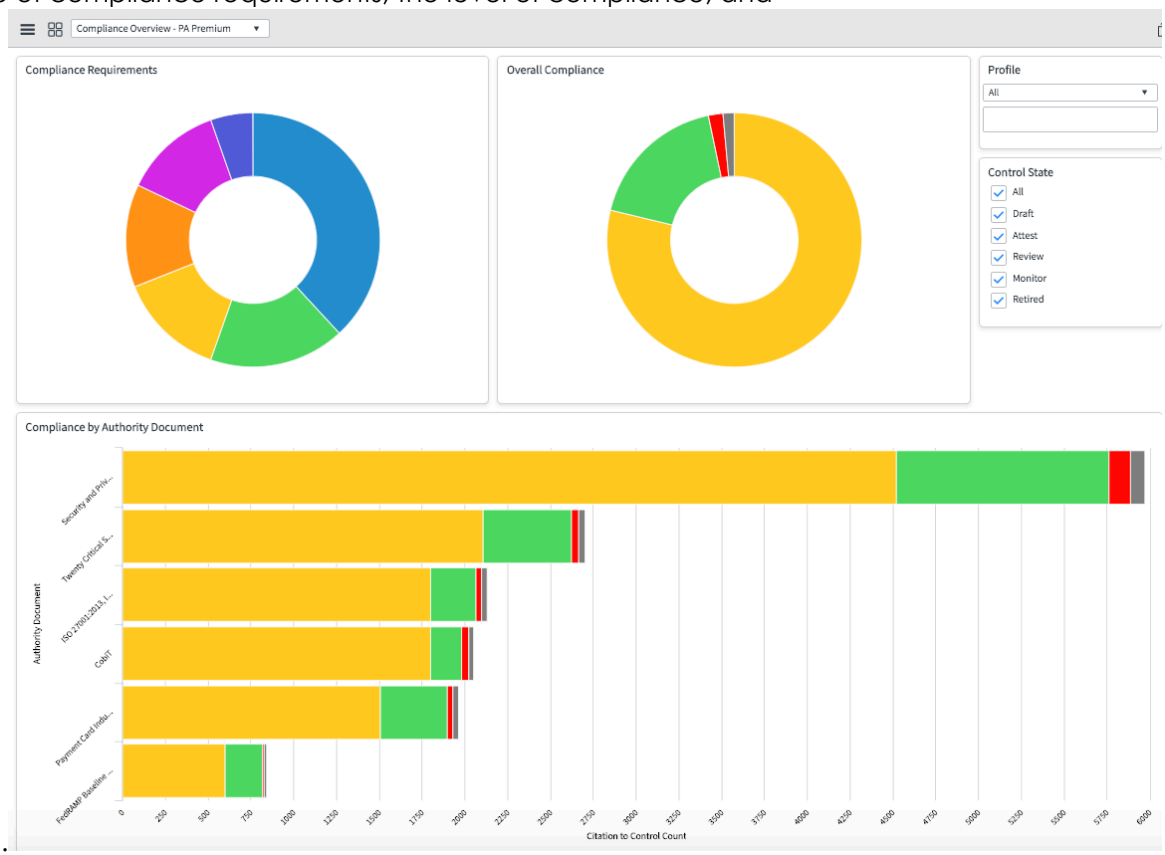
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## End users

| End user and goal | Required role |
|---|---|
| Audit Manager: Needs clear visibility into the overall state and volume of vulnerabilities within the organization. | sn_compliance.manager |
| Audit Administrator: Needs to pinpoint areas of concern quickly | sn_compliance.admin |
| Audit Analyst: Needs to quickly prioritize which risks/tasks to focus on based on criticality to the organization. | sn_compliance.user |

## Compliance Overview dashboard - PA Premium

The Compliance Overview dashboard provides views into the source of compliance requirements, the level of compliance, and trends.




## Reports

The Compliance Overview dashboard contains the following reports:

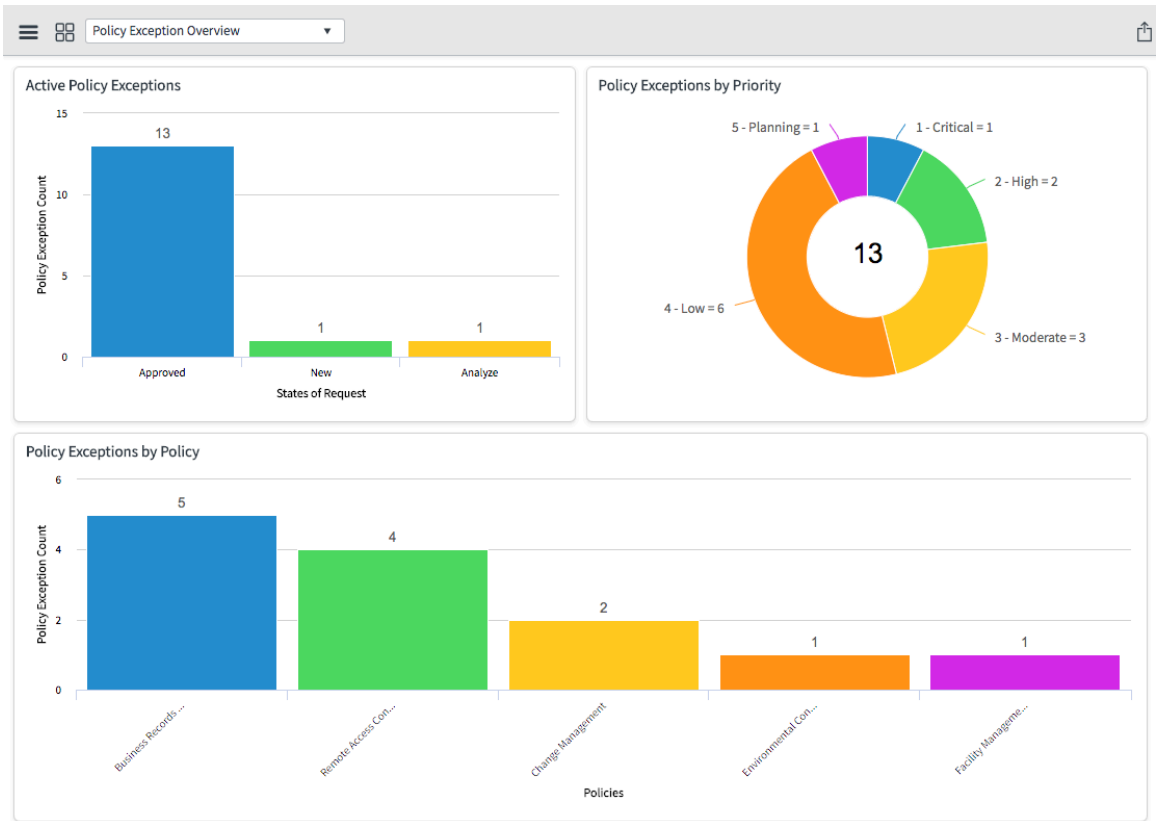
| Name | Type | Description |
|---|---|---|
| Compliance Breakdown | Multilevel Pivot | Citations are records with the specific requirements cited by an authority document. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Name | Type | Description |
|---|---|---|
| Compliance by Authority Document | Horizontal bar | The regulations, certifications, frameworks, standards, and best practices that an organization chooses or is required for compliance with regulations. |
| Compliance Requirements | Donut | The number of open requirements by authority document |
| Compliance score by department | Bar | Overall (average) compliance score by assignment group/ department |
| Compliance score trends | Box | Overall compliance by Authority Document |
| Overall Compliance | Donut | Overall compliance percentage of Citation Authority Document |

## GRC Policy Exception Overview dashboard

The Policy Exception Overview dashboard provides views into the number, severity, and source of policy exceptions. It also shows exempted controls.




## End users

| End user and goal | Required role |
|---|---|
| Audit Manager: Needs clear visibility into the overall state and volume of vulnerabilities within the organization. | sn_policy.manager |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| End user and goal | Required role |
|---|---|
| Audit Administrator: Needs to pinpoint areas of concern quickly | sn_policy.admin |
| Audit Analyst: Needs to quickly prioritize which risks/tasks to focus on based on criticality to the organization. | sn_policy.user |

## Reports

The Policy Exception Overview dashboard contains the following policies:

| Name | Type | Description |
|---|---|---|
| Active Policy Exceptions | Bar | Number of active exceptions against open policies |
| Approved Policy Exceptions | List | Number of total approved policy exceptions |
| Exempted Controls | List | List of controls that have exempt status |
| Exempted Controls Risks | List | List of control risks that have exempt status |
| Policy Exceptions | List | Policies are related to authoritative documents and control records. Publishing and version control of policies are managed using document and knowledge management capabilities from the Now Platform. Custom workflows ensure that all policy changes are routed to the appropriate work owners for final approval. All approved organizational policies are published in the knowledge base. |
| Policy Exceptions by Department | Bar | Total number of policy exceptions broken down by department |
| Policy Exceptions by Policy | Bar | Total number of policy exceptions broken down by policy |
| Policy Exceptions by Control Objective | Horizontal bar | Total number of policy exceptions broken down by control objective |
| Policy Exceptions by Priority | Donut | Total number of policy exceptions broken down by priority |
| Policy Exceptions by Entity | Horizontal bar | Total number of policy exceptions broken down by entity |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Privacy Management

Use the Governance, Risk, and Compliance: Privacy Management application to help protect your customers, employees, and suppliers with integrated data privacy risk and compliance management solutions and privacy by design concepts.

The Privacy Management application helps you to manage multiple privacy regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Australian Privacy Act. It also helps you to manage frameworks such as the National Institute of Standards and Technology (NIST), ISO 27001, and so on. The Privacy Management solution enables you to implement privacy policies and acknowledgments to handle the personal data of customers and employees.

| | | |
|---|---|---|
| Explore<br>  <br>Learn about how privacy managers, privacy users, and privacy administrators use the Privacy Management application. | Configure<br>  <br>Configure your Privacy Management application. | Use<br>  <br>Work on creating privacy assessments, processing activities and so on. |
| Analytics and Reporting<br>  <br>Highlight the privacy records with dashboards and reports. | Reference<br>  <br>Get details about components like tables and roles. | |

## Exploring Privacy Management

The ServiceNow® Privacy Management application enables you to manage your company's privacy programs. Some examples of privacy programs are privacy regulatory compliance programs, privacy impact assessments, privacy policy management, and so on.

All organizations collect personal data of customers, employees, and third parties in some form. Some examples of personal data are as follows:

- Home address
- Location data
- Identification card number
- Biometric data

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When your organization collects personal data, the data is exposed to multiple risks such as using the personal data for an organizational purpose without taking consent from the owners and the data getting inadvertently leaked. These events lead to compliance failure. Failure to manage data privacy laws can result in heavy fines and loss of customer and employee trust. This failure to protect data can also impact brand reputation.

The Privacy Management application helps you to manage multiple privacy regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Australian Privacy Act. It also helps you to manage frameworks such as the National Institute of Standards and Technology (NIST), ISO 27001, and so on. The Privacy Management solution enables you to implement privacy policies and acknowledgments to handle the personal data of customers and employees.

The following are the key capabilities to help you manage your organization's privacy programs effectively:

- Creating an inventory of critical business processes, applications, and vendors for privacy assessments.
- Setting up the privacy library content such as authority documents, citations, control objectives, risk statements, and policies.
- Managing privacy impact assessments.
- Managing privacy risk assessments.
- Discovering processing activities that process personal information.
- Managing processing activities to track their risk and compliance posture with continuous monitoring and issue management capabilities.
- Understanding and analyzing the overall privacy posture of your organization with various dashboards and reports.

The Privacy Management application is available on the Privacy Workspace. This workspace displays Home page, the Tasks page, the Issues overview page, and the List view. Every item on and inside these pages and lists are only specific to the Privacy Management application. This means that, for example, if you view citations and authority documents, they are specific to Privacy Management.

The Privacy Management solution is available as an add-on in the Integrated Risk Management (IRM) suite.

## Processing activities

A processing activity is a record that processes personal data. Examples of such records can be a business process or a business application of an organization that has personal information. Processing activities enable the privacy management teams to understand how personal information is being processed or used.

To manage the privacy programs, use any business process or business application that is available as inventory or records in the Configuration Management Database (CMDB) to create a processing activity record. Each business process or an application is a separate processing activity. After the privacy teams understand how personal data is being used, they can work with the business owners who own the processing activity and help them to be compliant with the necessary privacy regulations.

A processing activity stores the following type of information:

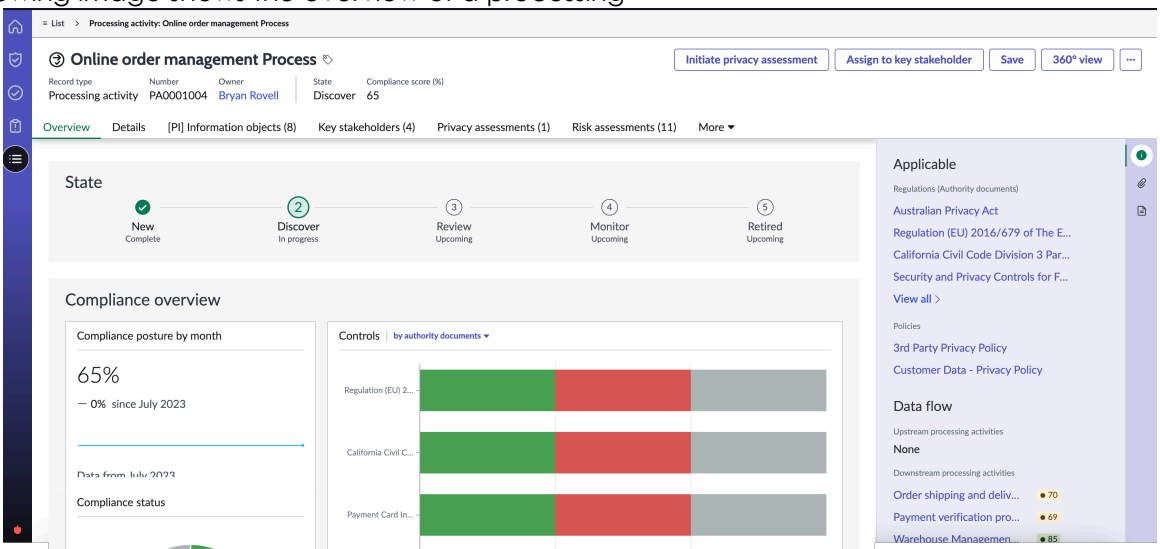
- Name and contact information of the data controller and the data processor.
- Purpose for which a processing activity is processing personal data. For example, lawful basis, legal obligations, and so on.

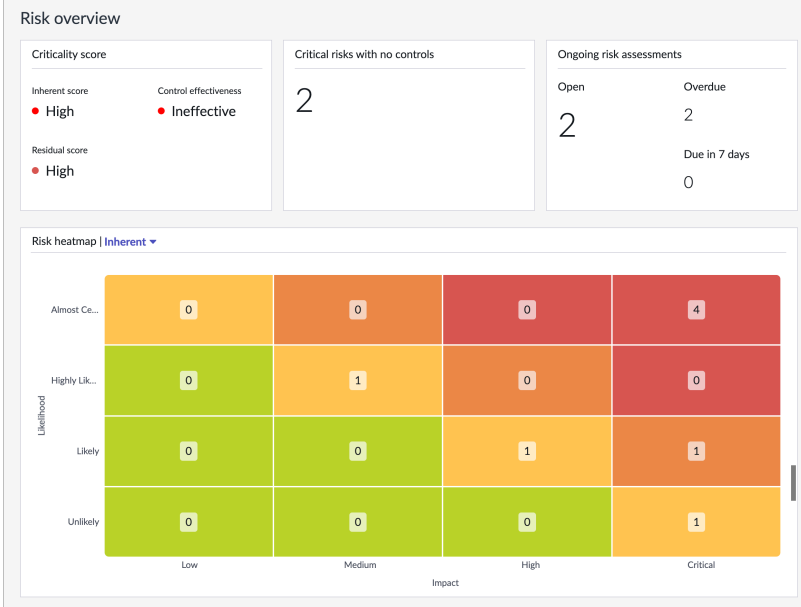
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

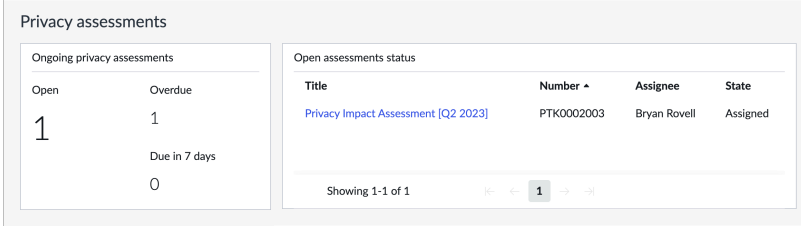
- Categories of data subjects and categories of personal data being processed. Examples of data subjects are customers or employees.
- Recipients with whom personal data is shared. For example, vendors or third parties and internal systems.
- Third parties in other countries and international organizations that receive the personal data.
- Privacy regulations, policies, risks, controls, and issues related to each processing activity.
- Key stakeholders of the processing activity such as the entity owners and others who are involved in the processing activity.

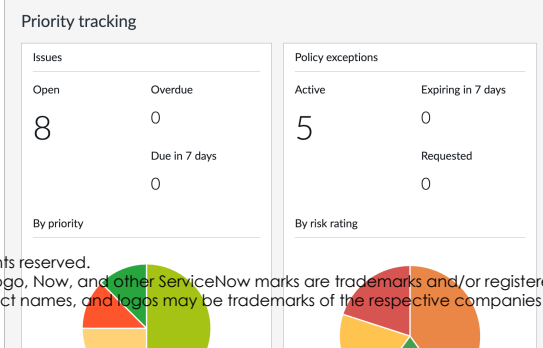
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following image shows the overview of a processing




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** The policies and controls that appear on the **Overview** page of the processing activity are specific to Privacy Management.

## Privacy assessments

Privacy assessments are used to collect information from business owners. This information helps the privacy teams to understand how personal information (PI) is being used or stored in a processing activity.

Using the privacy assessment capability, you can configure various types of assessments and send those assessments to the business process or business application owners to collect their responses. Some examples of the assessments that you can configure are as follows:

- Privacy screening initial assessments
- Privacy impact assessments (PIA)
- Privacy readiness assessments

When a privacy assessment is initiated, the business owners respond to the questions in the assessments. Their responses automatically create processing activities in the system. The necessary controls and information objects are then automatically mapped to the processing activities.

The privacy assessment capability provides multiple configurations options such as:

- Configuring various types of questions using a simple user interface.
- Configuring the creation of processing activities using the responses of the assessments.
- Mapping controls to question responses to determine the responses that will automatically map controls to the processing activities.
- Configuring [PI] Information objects for responses to automatically map the information objects to a processing activity. For more information, refer to Information objects in Privacy Management.
- Mapping question responses to processing activity fields to automatically fill the required data in the processing activity.

## Information objects in Privacy Management

Using information objects you can automatically discover business processes, applications, and third parties processing personal information.

The purpose of an information object is to logically describe the type of data that is exchanged between an application and a database. To determine which information objects process personal data, you can tag the information objects with the **Personal information** tag. For more details on how to tag an information object, see Tag an information object with personal information.

After the information objects are created, they are mapped to business applications or business processes. This activity helps the privacy management teams to discover the information objects processing personal data. Some examples of [PI] Information objects in Privacy Management are:

- Customer email addresses
- Customer bank account numbers
- Employee educational details
- Employee personal email address

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Creation of information objects

While you can manually create information objects, you can also use the BigID Data Exchange application to automatically identify personal information that is stored in your database and create information objects. You can download the BigID Data Exchange application from the ServiceNow Store.

## Privacy Workspace for the privacy manager

The privacy manager develops and maintains company policies and regulations.

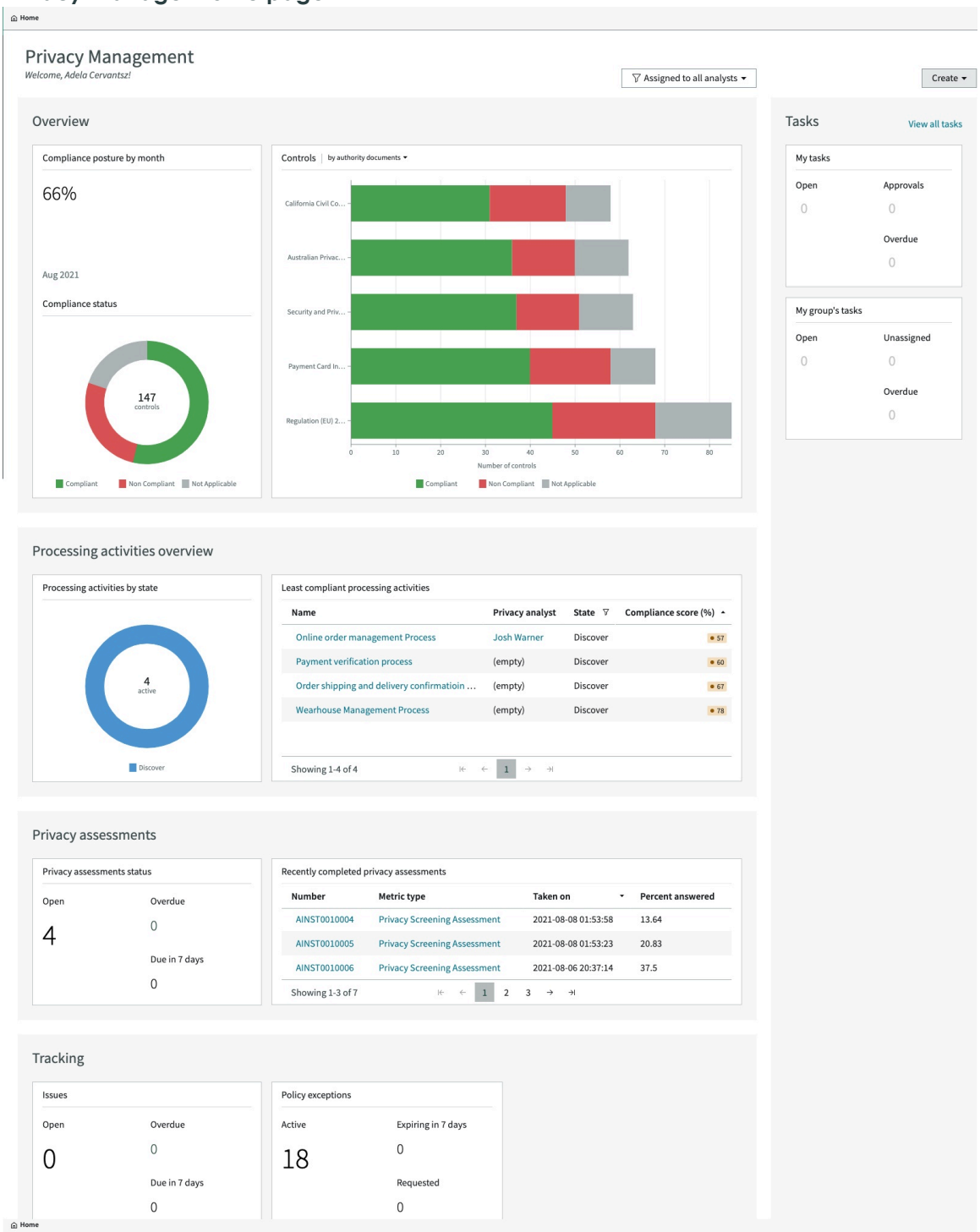
A privacy manager has the sn_privacy.manager role. Privacy managers do the following:

- Manage and monitor the overall organization-level privacy risk and compliance posture. The risk and compliance posture refers to the overall risk and compliance status of an organization across business processes, or business applications, and so on based on the risk scores, and compliant and non-compliant status of controls across various regulations.
- Develop and implement privacy regulations, authority documents, policies, and privacy risk statements.
- Review privacy regulatory requirements and policies.
- Design and monitor risks and controls to deal with breaches of privacy regulations and internal policies.
- Plan privacy programs and scope entities.
- Create privacy impact assessment templates.
- Perform privacy risk assessments to understand the criticality of the processing activities.
- Continuously monitor control effectiveness and recommend effective improvements.
- Supervise the privacy compliance team.
- Report the compliance posture to management and the board of directors.

The following image shows the Home page for the privacy manager.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Privacy manager home page




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Privacy Workspace for the privacy analyst

Privacy analysts manage the privacy compliance posture of the processing activity owned by them. Compliance posture refers to the overall compliance status of an organization, business process, or business application, and so on based on the compliant and non-compliant status of controls across various regulations.

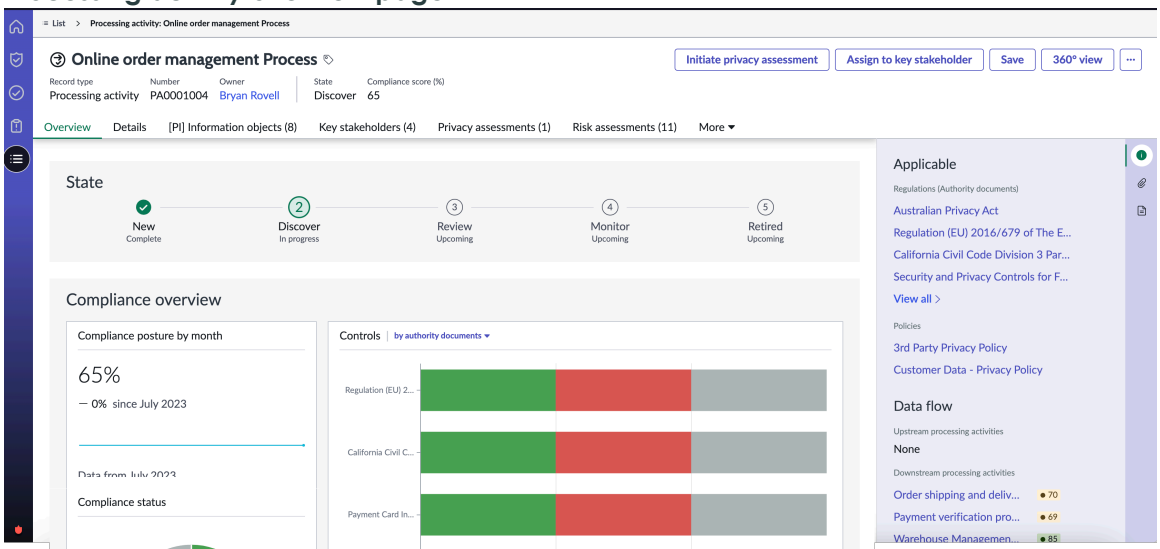
A privacy analyst has the sn_privacy.analyst role. The primary tasks for a privacy analyst are as follows.

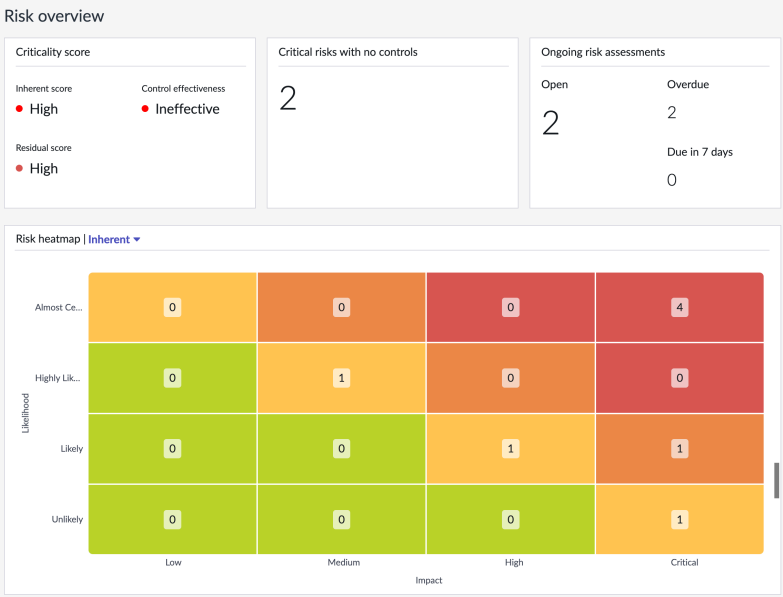
- Assess the processing activities regularly by sending and reviewing privacy impact assessments.
- Work with the management and business users to identify and manage controls related to a processing activity.
- Manage and resolve the concerns of business users about compliance-related issues and policy exceptions.
- Test and monitor control effectiveness.

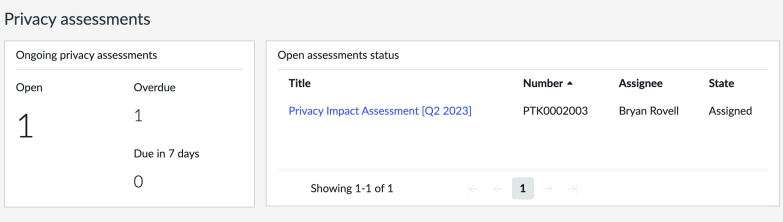
The following image shows the processing activity overview page for the privacy analyst.

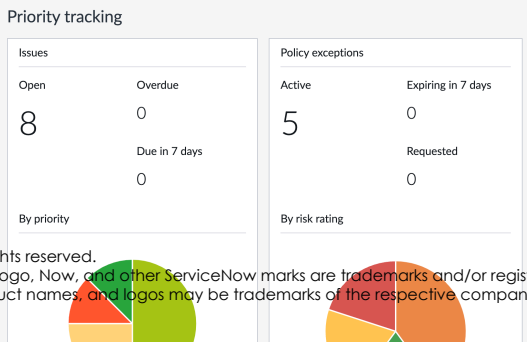
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Processing activity overview page




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

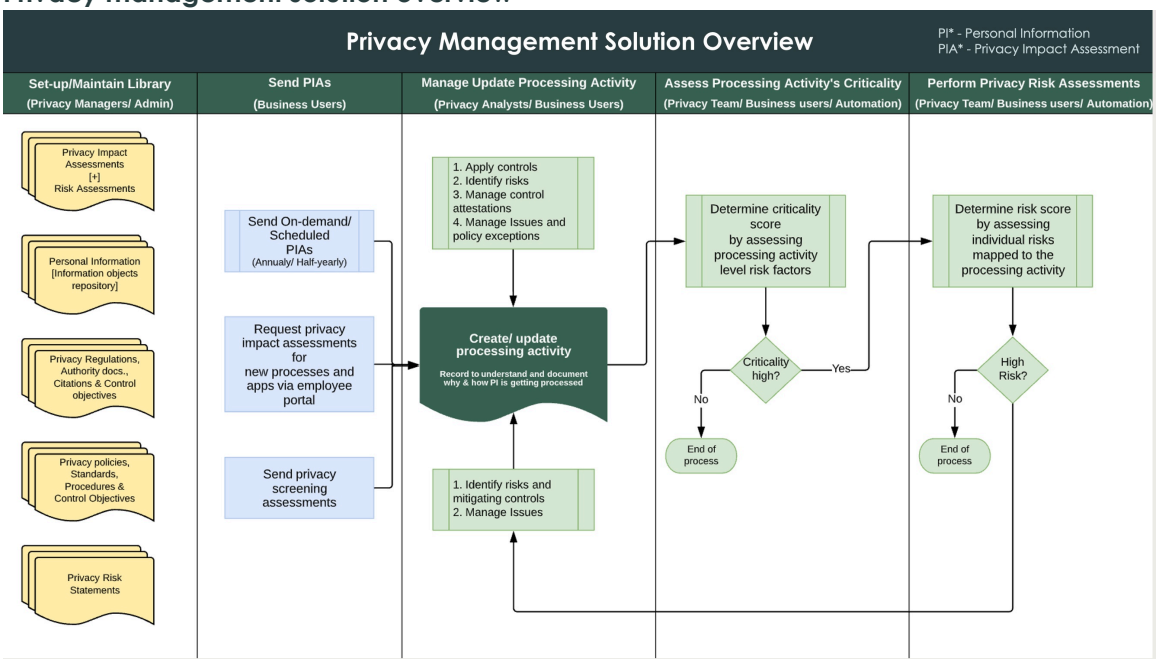
## Privacy Management solution overview

The Privacy Management solution provides you a framework to manage your privacy-specific libraries such as citations, policies, control objectives, risk statements, privacy impact assessments and privacy risk assessments. It also provides processing activity records to track the privacy risk and compliance posture for a business application or a business process by applying and monitoring the relevant risks and controls.

Before planning your privacy program, ensure that you set up the privacy libraries according to the privacy regulations that you plan to implement. For more information on the library setup, refer to Manage the Privacy Management library.

The following figure demonstrates the Privacy Management solution.

**Privacy management solution overview**




The Privacy Management solution is described as follows.

## Create a library

As a privacy manager, with the role sn_privacy.manager, or privacy administrator, with the role, sn_privacy.admin, you must set up your libraries using the following.

- Privacy impact assessments
- Personal information objects
- Privacy regulations, authority documents, citations, and control objectives.
- Privacy policies and procedures
- Privacy risk statements

## Privacy impact assessments

1. Discover inventory: As a privacy manager, with the role sn_privacy.manager, identify or discover the inventory such as business processes, business applications, vendors, and business services that process personal data. All such inventory is stored in the respective Configuration Management Database (CMDB) tables. The respective business owners manage the inventory. As a privacy manager, use the Entity types feature and create an

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

entity for each inventory record. For more information about entity types, see Exploring the entities. At this stage, based on the discovery method, you can use one of the following approaches to create processing activities.

a. Search business processes or applications that process personal data: Use this approach when business processes, applications, services, or vendors are associated with information objects. Using the entity type functionality, search for entities that process [PI] Information objects. Based on the search results, directly create the processing activity records. This approach is used only when the business owners associate the inventory with information objects. For more information, see Entity scoping to plan a privacy program.

b. Send privacy screening assessments: Use this approach when information objects are not associated with the inventory such as business applications and processes. In this approach, send privacy screening assessments to the respective business owners. These screening assessments contain basic questions. Some examples of the questions are as follows:

   - Are you processing personal information as a part of the business process or application that you own?
   - What kind of personal information you are processing? For example, email, phone, and address.

   If the assessment responses determine that there is personal data, processing activities are created automatically.

2. Business users can proactively submit privacy impact assessments for new applications and processes from the Employee Center.

## Manage and update the processing activities

1. Create or update a processing activity: As a privacy analyst, with the role sn_privacy.analyst, send a privacy impact assessment (PIA) to the processing activity or business owners after a processing activity is created. The privacy impact assessment helps to understand why and how the processing activity processes personal information. The assessment collects information such as justification for storing PI data, exchange of PI data with other systems, and the security of PI data.
2. Send or automatically initiate PIA: As a privacy analyst, send a privacy impact assessment (PIA) from a processing activity whenever you must collect more information. Alternatively, you can also automatically initiate the assessments based on the privacy program frequency defined by the privacy manager and the privacy administrator. An auto-initiate schedule can be created using the Now Platform capabilities.
3. Apply risks and controls related to the processing activity: As a privacy analyst, after you understand how personal information is being used in the processing activity, the necessary risk statements, controls, policies, and authority documents are automatically applied to the processing activities based on the assessment responses. For more information on how to configure assessments, see Create an assessment template. After the controls are added, the privacy analyst can review the controls and add or remove the controls as necessary.
4. Send control attestations: After the final set of controls is associated with the processing activity, the control attestations are sent to the business process owners or the application owners to collect the evidence for every control that is applied. When the business owners respond to control attestations with evidence for each control, compliant and non-compliant controls are identified. This identification determines the compliance posture of the processing activity.
5. Report and monitor issues: Issues are created automatically for non-compliant controls and are assigned to their respective business owners. The privacy analyst monitors the issues.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Manage issues: To manage issues, business owners can do one of the following:
   - Resolve the issue: Resolving the issue makes the control compliant.
   - Raise a policy exception: An exception is raised for an issue that cannot be resolved immediately. Privacy analysts can review the policy exceptions and can either accept or reject the exceptions based on the criticality of the issue.
7. Continuous control monitoring: Privacy analysts continuously monitor the controls on a processing activity using the indicator functionality. For more information about indicators, see Risk indicators, control indicators, and indicator templates.

## Assess the criticality of processing activities

The criticality score provides the risk posture at the processing activity level by assessing the factors at processing activity-level. When a processing activity is created or updated, a criticality assessment is performed on the processing activity to understand the high-level risk score or the criticality score.

## Perform privacy risk assessments

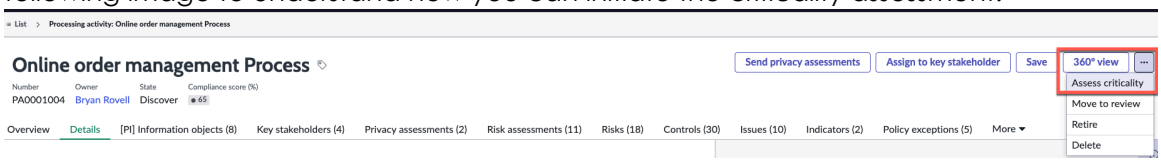
Privacy risk assessments are detailed assessments that are conducted if the criticality score is high. Assess each risk that is associated with the processing activity and know the aggregated risk score on the processing activity. After you assess the privacy risks, you can view the privacy risk posture on the risk heatmap in the overview section. The heatmaps provide detailed information about your inherent and residual risks.

## Risk assessments in Privacy Management

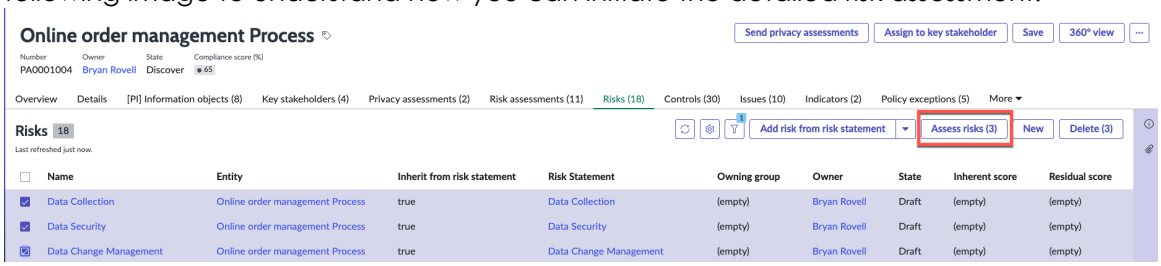
You can perform risk assessments on your processing activities to determine their risk scores and find out the privacy risk posture of your organization.

To understand the risk posture, the following assessments that are performed.

- **Criticality assessment**: Provides the risk posture at the processing-activity level by assessing the factors at processing activity-level. When a processing activity is created or updated, a criticality assessment is performed on the processing activity to understand the high-level risk score or the criticality score. See the following image to understand how you can initiate the criticality assessment.



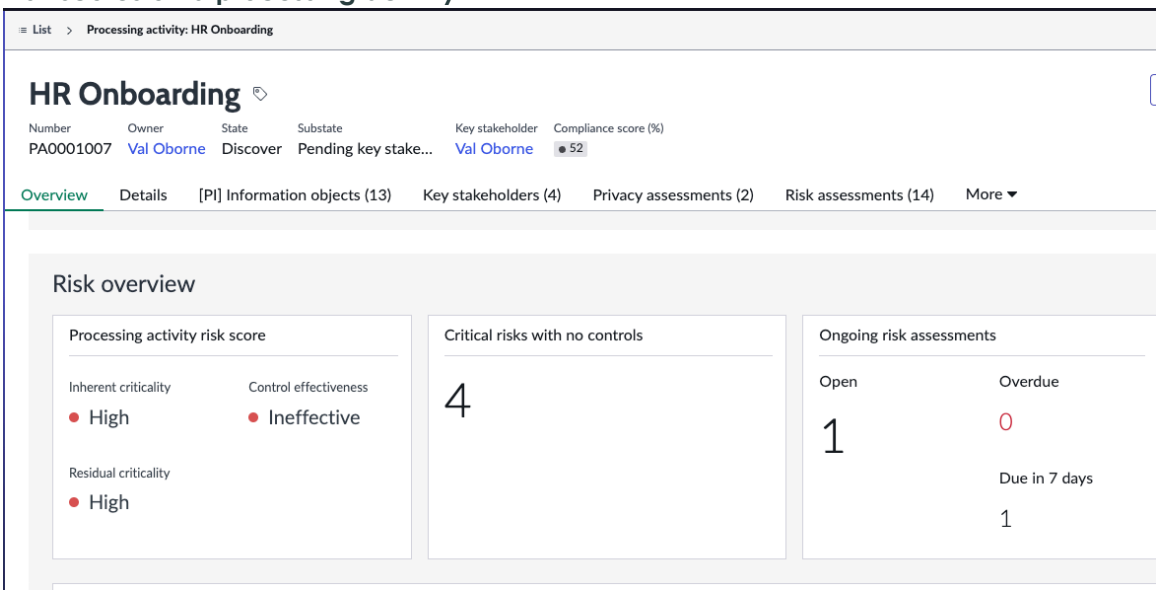

- **Privacy risk assessment**: Privacy risk assessments are detailed assessments that are conducted if the criticality score is high. Assess each risk that is associated with the processing activity and know the aggregated risk score on the processing activity. After you assess the privacy risks, you can view the privacy risk posture on the risk heatmap in the overview section. The heatmaps provide detailed information about your inherent and residual risks. See the following image to understand how you can initiate the detailed risk assessment.



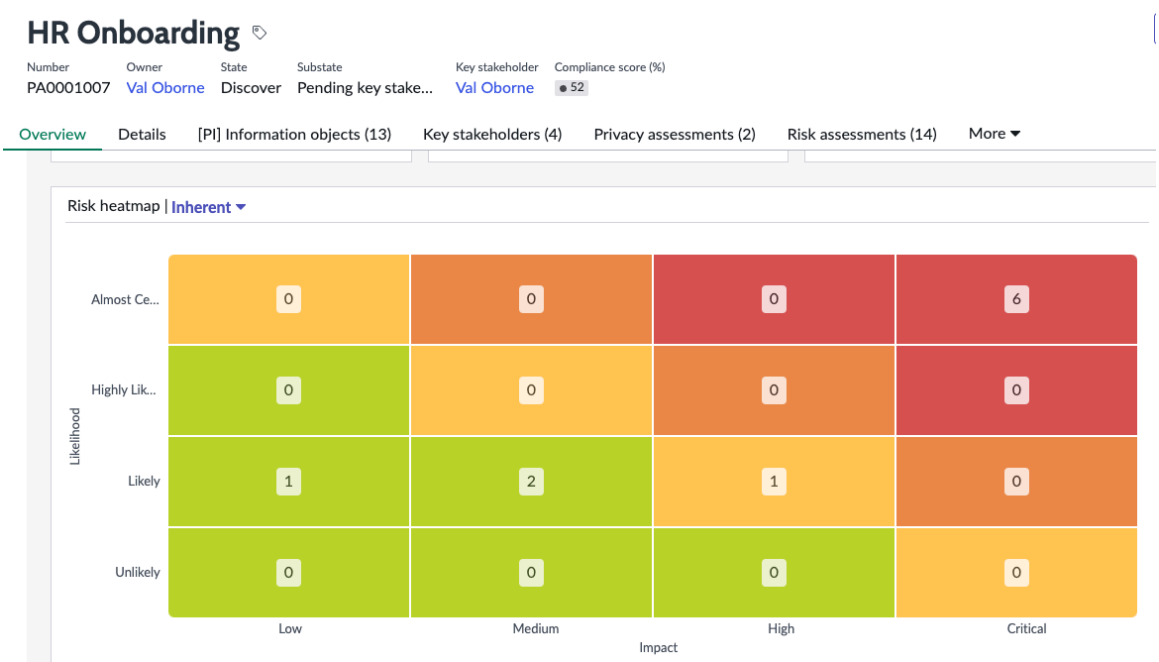

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The risk assessments results and the risk heatmaps appear on the processing activity home page as shown in the following image.

### Risk scores on a processing activity




### Risk heatmap on the processing activity




To understand the details about how to perform the risk assessments, see Privacy assessment configurations.

### Privacy assessment configurations

To perform a processing activity criticality and privacy risk assessment, two risk assessment methodologies (RAMs) are provided by default.

The RAM is a configuration or a record in the risk assessment engine. It is a part of the Advanced Risk application. The RAM is used for assessing either the risks or objects in your organization. A configured RAM is an object with associated assessment types that have associated factors. This allows an organization to have different methodologies for assessing

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

risk. To understand more about the factors or questions used in the assessments, refer to Factors in Advanced Risk Assessment.

The privacy-specific RAM records have the **Domain** field set to **Privacy**. As a privacy administrator, you can make a copy of the default RAMs and modify them. To understand more about RAM configurations, refer to Configure a risk assessment methodology. To understand how you can make a copy of a RAM, refer to and Copy a risk assessment methodology.

It is important to consider the following points when performing risk assessments.

- In the **Privacy** domain, you can only modify a RAM. Creation of a RAM is not permitted.
- Only two active RAMs are allowed. If you must copy or modify more than two RAMs, you must retire one.
- The RAM can be configured and its order can be modified according to your requirements.
- Users with the following roles can perform the privacy-related criticality and detailed privacy risk assessments.
  - Privacy business user (sn_privacy.business_user)
  - Privacy analyst who owns the processing activity
  - Privacy assessment responder (sn_privacy.assessment_responder)
  - Privacy manager (sn_privacy.manager)

## Configuring Privacy Management

Follow the order of the tasks given here to configure Privacy Management. These tasks will help you manage your privacy program effectively.

### Download Privacy Management

Before you run GRC: Privacy Management (sn_privacy) in your instance, you must download it from the ServiceNow Store.

**Before you begin**
Role required: admin

**Procedure**

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

### Manage the Privacy Management library

The Privacy Management library consists of authority documents, citations, control objectives, policies, and [PI] Information objects that help to manage the privacy content.

### Authority documents

Authority documents are the principles, guidelines, regulations, standards, and frameworks that organizations must comply with. Some examples of authority documents are:

- Statutes (Bills or Acts)
- Regulations
- Audit Guidelines

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Organizations can either create the authority documents, citations, and control objectives or they can download and import them from a third-party provider such as the Network Frontiers Unified Compliance Framework (UCF).

## Citations

Citations are records with the specific requirements cited by an authority document. A citation relates authority documents to its applicable controls. Each citation has control objectives.

## Policies

Policies include control objectives. Policies can also be associated to authority documents. Policies are published and regularly updated with incremented versions. For more information on policies, refer to Policy and Compliance Management.

## Risk statements

Using risk statements you can create a central risk register to manage potential privacy risks that may occur any time and any where in an organization.

## Privacy assessments

Privacy assessments are used to collect information from business owners. This information helps the privacy teams to understand how personal information (PI) is being used or stored in a processing activity.

## Risk assessments

The risk assessments capability enables you to determine the organizational privacy risk posture using criticality and privacy risk assessments.

## PI Information objects

[PI] Information objects refer to information objects that are of type **Personal information**. To understand the benefit of using information objects in the Privacy Management solution, refer to Information objects in Privacy Management. Maintaining a library of [PI] Information objects and associating them with the processing activities helps the privacy teams to understand what personal information (PI) is being processed by the processing activity.

Only the information objects that are tagged with the **Personal information** tag are available to be added to a processing activity. For more information on how to tag information objects see, Tag an information object with personal information.

### Tag an information object with personal information

Categorize information objects to use in the Privacy Management solution with the personal information tag. Only tagged information objects can be associated with the processing activities.

**Before you begin**
Role required: sn_privacy.manager

**About this task**
Information objects that are tagged with personal information can be used in the privacy assessments and processing activities.
Even if you create a new information object from the **[PI] Information objects** list view, you must add a Personal information tag to them. Do not assume that because you are

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

creating an information object in the [PI] Information objects list, the information object is automatically tagged.

### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace**.
2. In the Privacy Workspace, click the List icon ( ).
3. Navigate to **Information objects** > **All Information objects**.
4. Select and open the information object you want to tag.
5. Select the tag icon ( ).
6. In the Tag window, type `Personal information` and select the option that appears.
7. Click **Save**.

### Result

The information object that you tagged with personal information appears in the [PI] Information Objects list.

## Create a privacy assessment

Create various types of assessments and send those assessments to the business process or business application owners to collect their responses. The responses help you to understand how personal information (PI) is being used or stored in a processing activity.

### Before you begin

Role required: sn_privacy.admin and sn_privacy.manager

### About this task

Using the privacy assessment capability, you can create various types of assessments such as privacy screening initial assessments, privacy impact assessments (PIA), and privacy readiness assessments.
The following capabilities are provided to configure the assessments:

- Mapping control objectives to the responses of the question.
- Mapping information objects to the responses of the question.
- Mapping the processing activity fields to the responses of the questions.

While configuring the assessments, consider the following terminology:

- Metric type refers to the assessment template.
- Metric category refers to the section label in the assessment.
- Metric refers to a question.

### Procedure

1. Navigate to **All** > **Privacy Management** > **New Assessment Template**.
2. On the form, fill in the fields.

#### Assessment Metric Type form

| Field | Description |
|---|---|
| Name | Name of the assessment template. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Assessment duration | Length of time allowed for completing the assessment from the time the assessment is generated. |
| Table | Table that contains the records. |
| Auto approve privacy assessment tasks | Option to indicate that the privacy assessment tasks must be automatically approved without a review. When this option is selected, after the assessment task is submitted, automatically the assessment task is approved and controls, risks and the information objects are created on the processing activity, and the task is closed. |
| State | State of the assessment. This field is automatically set to **Draft**. |
| Roles | Roles that have read access to the template. |
| Classification | Classification of assessment metric type. The choices are the following:<br>◦ **None**<br>◦ **Initial Assessment**<br>◦ **PIA Assessment** |
| Description | Purpose of the assessment template and the reason for its creation. |
| Introduction | Guidance text for business users who respond to the assessment. |

3. Click **Save and Open Designer**.
   The designer contains the following elements.

| Element | Description |
|---|---|
| Controls | Supported question data types that are available in the Controls palette. |
| Questions | Library of questions for various categories. |
| Categories | New assessment opens in the Design view. The questionnaire **Name** field appears above the first category in the canvas. An empty question field appears in the category container. |

4. Drag a control on the designer canvas to create a question of that type.

   The canvas contains the following types of questions controls.

### Question controls

| Data type | Description |
|---|---|
| Attachment | Questions that enable users to attach one or more files as a response. |
| Boolean | Questions with the following value types:<br>◦ A check box to select or clear.<br>◦ A Yes or No answer. |
| Choice | Questions with a list of predefined options. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Data type | Description |
|---|---|
| Date | Date field. Enables you to collect the date information filled in by a respondent. |
| Date/Time | Date and time field. Enables you to collect the date and time information filled in by a respondent. |
| Number | Number field with predefined minimum and maximum values. The default range is 1–10. |
| Percentage | Percentage field with a prescribed range. |
| Scale | Predefined Likert scale. Answer options appear as radio buttons. |
| Numeric Scale | Numeric or numerical scale. Requires the respondent to provide the response in terms of numerical values. |
| String | Single or multi-line text field. |
| Template | List of templates that provide a predefined scale of options. |
| Reference | List of fields from a specified reference table. |
| Image Scale | Image question. Enables you to click images as your answer to a question. |
| Multiple Selection | Multiple options. You can select multiple options as responses. |
| Ranking | Question type with options as answers. The options must be ranked. |

5. Point to **Save** and then click **Save and Publish**.
   The state of the template changes to Published.

### Result
The assessment template with the questions is ready to be sent to the entity owner.

### What to do next
Map the assessment responses to a processing activity. For more information, see Map the processing activity fields to a question response.

#### Write a processing activity script

Write custom scripts on the assessment templates to update the processing activity fields using a script. The script runs when the assessment response is completed. You can write multiple scripts for both screening assessments and impact assessments.

### Before you begin
Role required: sn_privacy.developer

### Procedure

1. Navigate to **All** > **Privacy Management** > **Assessments** > **All Assessment Templates**.
2. Open the assessment template for which you want to write the script.
3. Select the Processing activity script configurations related list.
4. Select **New**.
5. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Processing activity script configuration form**

| Field | Description |
|---|---|
| Name | Name of the script. |
| Assessment template | Assessment template to use. This field is automatically set. |
| Active | Option to indicate if the script is active. An active script is executed when the assessment response is submitted and the processing activity is created.<br>**Note:** Only one script can be marked as active at a time. |
| Description | Script description. |
| Script | Script to be used to update the processing activity. |

6. Select **Submit**.

### Map a control objective to a question response

Map the control objectives to the responses of the assessment questions to automatically create and apply the respective controls on the processing activity.

#### Before you begin

You can apply active and inactive controls to an assessment response. However, when an assessment is submitted by the business user, only the mapped control objectives that are in the **Active** state are considered to create and apply the controls on the processing activity.

Role required: sn_privacy.admin and sn_privacy.manager

#### About this task

You can relate control objectives to an assessment question only if the questions are of the following types:

- Choice
- Image scale
- Numeric scale
- Ranking
- Boolean
- Template

**Note:** For Boolean questions, the question can either use yes or no answers or use check boxes that must be selected or cleared.

#### Procedure

1. Navigate to **All** > **Privacy Management** > **Assessment Templates**.
2. Click and open the required assessment template.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Type of questions | Steps to map controls |
| --- | --- |
| Boolean, Template | To create and apply controls for a response, perform the following steps.<br>**a.** Select the response in the **User response to create controls** field.<br>**b.** From the Control Objectives related list, click **Edit**.<br>**c.** Double-click the required control objectives in the Collection list.<br>**Note:** Double-clicking automatically moves the objects to the Control objectives List list.<br>**d.** Click **Save**. |
| Choice, Image scale, Numeric, Ranking | To create and apply controls for a response, perform the following steps.<br>**a.** In the Metric Categories related list, click the required metric.<br>**b.** In the Assessment Metrics related list, click the required question.<br>**c.** In the Assessment Metric Definitions related list, select a value for which you want to map control objectives.<br>**d.** From the Control Objectives related list, click **Edit**.<br>**e.** Double-click the required control objectives in the Collection list.<br>**Note:** Double-clicking automatically moves the objects to the Control objectives List list.<br>**f.** Click **Save**. |

3. Click **Update**.

**Result**
The control objectives are related to the processing activity.

### Map an information object to a question response

Map the [PI] Information objects to the responses of the assessment questions that must be associated to the processing activity. This association helps the privacy teams to understand what personal information is being processed by the processing activity.

**Before you begin**
Role required: sn_privacy.admin and sn_privacy.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

You can relate information objects to an assessment question only if the questions are of the following types:

- Choice
- Image scale
- Numeric Scale
- Ranking

To understand more about information objects and their uses, see Information objects.

### Procedure

1. Navigate to **All** > **Privacy Management** > **Assessment Templates**.
2. Click and open the required assessment template.
3. In the Metric Categories related list, click the required metric.
   The metric category expands.
4. In the Assessment Metrics related list, click the required question.
5. In the Assessment Metric Definitions related list, select a value for which you want to map information objects.
6. From the Information objects related list, click **Edit**.
7. Double-click the required information objects in the Collection list.
   Double-clicking automatically moves the objects to the Information objects List list.
8. Click **Save**.
9. Click **Update**.

### Result

The information objects are related to the processing activity.

## Map a risk statement to a question response

Map the risk statements to the responses of the assessment questions to automatically create and apply the respective risks on the processing activity.

### Before you begin

Role required: sn_privacy.admin and sn_privacy.manager

### About this task

When a user responds to a question, based on the answers, the corresponding risk statement is mapped to the processing activity.
You can relate risk statements to an assessment question only if the questions are of the following types:

- Choice
- Image scale
- Numeric scale
- Ranking
- Boolean
- Template

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** For Boolean questions, the question can either use yes or no answers or use check boxes that must be selected or cleared.

### Procedure

1. Navigate to **All** > **Privacy Management** > **Assessment Templates**.
2. Click and open the required assessment template.
3. Open the question for which you want to add risk statement

| Type of questions | Steps to map risk statements |
|---|---|
| Boolean, Template | To create and apply risk statements for a response, perform the following steps.<br>**a.** Select the response in the **User response to create controls** field.<br>**b.** From the Risk Statements related list, click **Edit**.<br>**c.** Double-click the required risk statements in the Collection list.<br>**Note:** Double-clicking automatically moves the objects to the Risk statements list.<br>**d.** Click **Save**. |
| Choice, Image scale, Numeric, Ranking | To create and apply risk statements for a response, perform the following steps.<br>**a.** In the Metric Categories related list, click the required metric.<br>**b.** In the Assessment Metrics related list, click the required question.<br>**c.** In the Assessment Metric Definitions related list, select a value for which you want to map risk statements.<br>**d.** From the risk statements related list, click **Edit**.<br>**e.** Double-click the required risk statements in the Collection list.<br>**Note:** Double-clicking automatically moves the objects to the Risk statements list list.<br>**f.** Click **Save**. |

4. Click **Update**.

### Map the processing activity fields to a question response

Map some of the processing activity fields with the responses of the assessment questions to update the processing activity details based on the assessment response.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_privacy.admin

### About this task
A processing activity form has multiple fields. You can choose which responses of the assessment questions must be copied to the various fields of the processing activity record. For example, you can configure that if a certain question has Yes as an answer, then the short description of that question must be used in the **Name** field of the processing activity form.

The following table shows mappings between the fields on the processing activity form with the assessment template configurations:

| Field type in assessment configuration | Field labels on the assessment template configurations | Field labels on the processing activity form |
|---|---|---|
| String | Name | Name |
| String | Description | Processing activity purpose |
| String | Data retention period (in days) | Data retention period (in days) |

### Procedure
1. Navigate to **All** > **Privacy Management** > **Assessments** > **All Assessment Templates**.
2. Click and open the required assessment template.
3. In the Metric Categories related list, click the required metric.
   The metric category expands.
4. Click the question from which you want to copy the fields to the processing activity.
5. Click the **Processing Activity Configuration** section.
6. From the **Processing activity field** field, select the field that must be populated in the processing activity form.
7. Click **Update**.

## Create and validate an assessment configuration

Create your assessment configurations to determine when a processing activity must be automatically created.

### Before you begin
Role required: sn_privacy.admin or sn_privacy.manager

### About this task
When a privacy screening assessment is sent to the entity owners, their responses determine the creation of processing activity. You can also modify the default configurations on the privacy screening assessment to create processing activities automatically.
You can also create a new processing activity creation condition for your own privacy screening assessments.

After you create the configurations, you can validate if the responses create the processing activities according to the defined conditions.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Privacy Management** > **Assessments** > **Processing activity creation rules**.
2. Click **New**.
3. On the form, fill in the fields.

**Processing activity creation rule form**

| Field | Description |
|---|---|
| Name | Name of the assessment configuration. |
| Description | Brief description of the configuration. |
| Assessment template | Template for which the configuration is being created. |
| Active | Option to make the configuration active. |
| Advanced | Option to add more than three conditions. |

4. In the Conditions related list, create filters by selecting **Metric** and using the condition builder.
5. In the Advanced related list, specify the script for adding more than three conditions. The Advanced related list only appears if you select the **Advanced** option.
6. Click **Validate**.
   a. In the **Assessment instance** field, select the instance on which this configuration must be used.
   b. Click **Validate**.

## Map a table with a processing activity

Keep your processing activity updated and in sync with any table in ServiceNow® by mapping the entity fields with the processing activity.

### Before you begin

Role required: sn_privacy.analyst

### About this task

A processing activity is associated with a CMDB table record such as a business process record or a business application record. Whenever a CMDB record is updated, the respective processing activity must also be updated so that the privacy teams can apply the controls based on the updates to the processing activity. Using the **Sync fields** button on the processing activity form the privacy managers and analysts can update the processing activity. The processing activity is updated based on the configurations available in the processing activity mapping.

When the **Sync fields** button is selected, only the fields that are mapped with the processing activity are updated.

When mapping a **Processing activity field** with a **Mapping field**, it is important to note that the following mapping combinations are supported:

- String to String
- Reference type to the same Reference type
- True or False
- Integer to Integer and String

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Additionally, ensure that there is valid data for both the fields. For example, if there are filter conditions applied in the Processing activity field, these must match the filter conditions in the Mapping field.

### Procedure

1. Navigate to **All** > **Privacy Workspace** > **Configure privacy management** > **Processing activity mapping**.
2. Click **New**.
3. In the **Mapping table** field, select **Business Application**.
4. In the **Description** field, provide a brief description of the table.
5. Click **Save**.
   The Processing activity field mappings related list appears.
6. Click the Processing activity field mappings related list.
   a. Click **New**.
   b. In the **Processing activity field**, select the field of the processing activity form that you want to map with the business application table field.
   c. In the **Mapping field**, select the field of the business application table field that you want to map with the processing activity field.
   d. Click **Save**.

### Result

The mapping is successfully created. The fields that are mapped will be populated in the processing activity form.

## Using Privacy Management

As a privacy analyst or a privacy manager, you can identify which business applications or processes store and use personal information.

### Entity scoping to plan a privacy program

When a privacy manager plans the privacy program for an organization, the first step is to scope those business applications or processes that contain personal data. In Governance, Risk, and Compliance, these business applications or business processes are called as entities. After you identify the entities processing personal data, the processing activities are automatically created.

A privacy manager, with the role sn_privacy_manager, plans various privacy programs. Some examples of the privacy programs are:

- Identifying all the business processes and vendors that process personal data of customers.
- Identifying business applications that process personal data of employees.

All the inventory related to business processes, applications, vendors, or business services is stored in the respective Configuration Management Database (CMDB) tables. The respective business owners manage this inventory.

You can identify or discover entities that process personal data by using one of the following methods.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Filtering the entities either by discovering the processing activities by their usage of personal information.
- Sending initial privacy assessments.

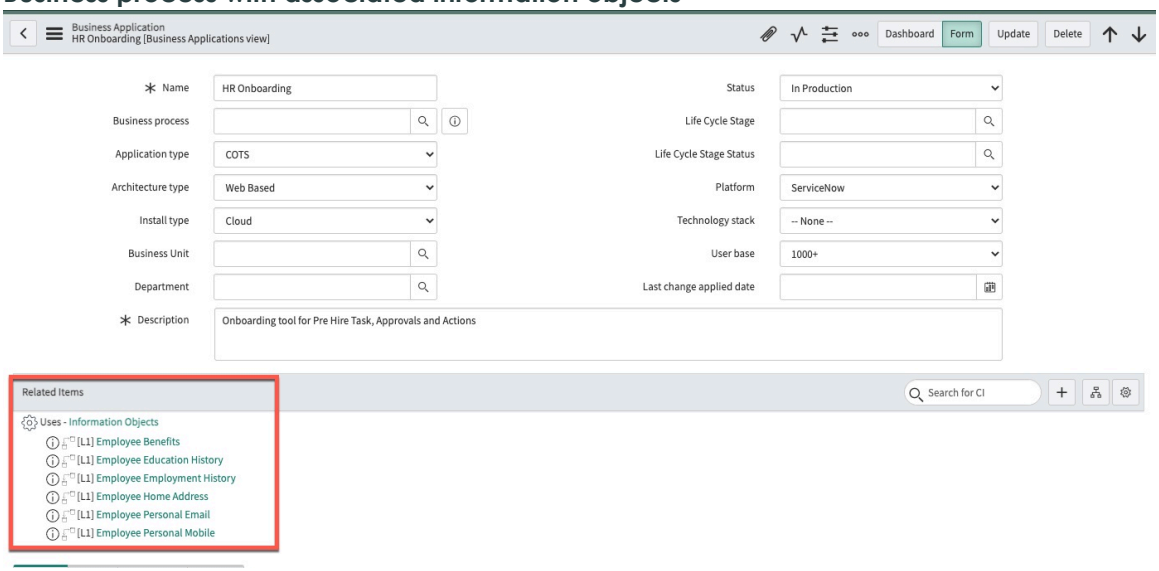
Both these methods are explained in the following sections.

Discover processing activities by their usage of personal information

At an inventory level, when business processes, business applications, and other inventory records are mapped with information objects of type Personal information (PI), the privacy manager can discover those records that process specific PI information. For details about information objects and their role in Privacy Management, see Information objects in Privacy Management.

The following image shows a business process with information objects associated with it. To identify such business applications or processes associated with information objects, the enhanced entity filter capability in the entity scoping functionality is used. For more information, see Scope entities to discover processing activities with personal information.

**Business process with associated information objects**



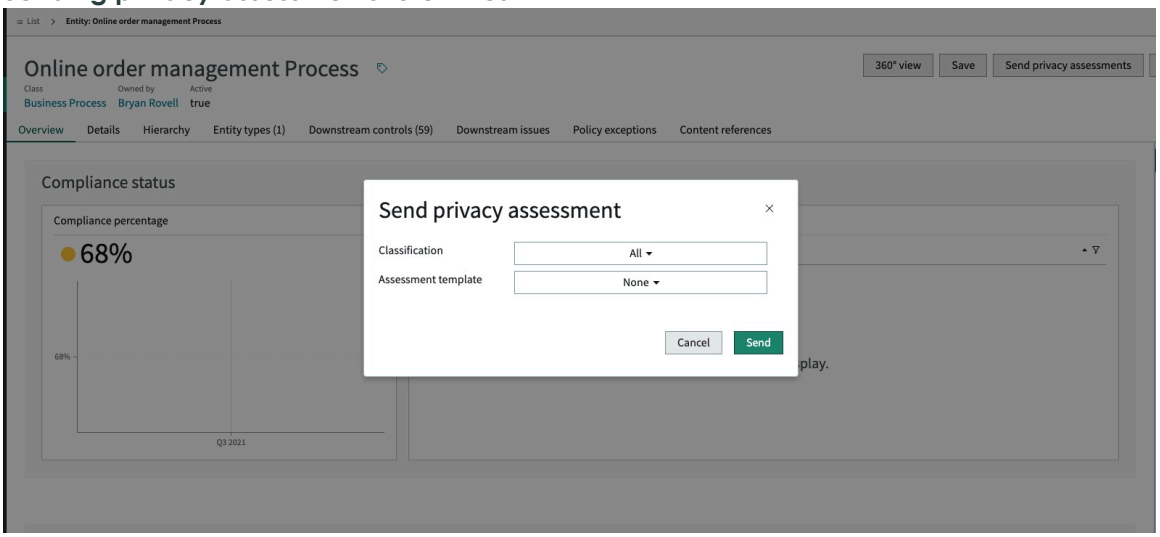

Identify potential entities and sending initial privacy assessments

If the information objects are not mapped to the business applications or processes, you can send initial privacy assessments to all the entities and use their responses to determine if personal data is being processed. The steps to send the assessment are as follows:

1. Create an Entity type. For example, `Business processes that process customer personal information` or `Business applications that store employee information`.
2. Identify entities using Entity Type you created.
3. Select the relevant entities and send privacy screening assessments to the respective entity owners.
4. Based on the responses, processing activities are created automatically when relevant questions are answered.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Sending privacy assessments to entities




After the entities are scoped, then, in the applications, only those entities appear that contain personal information.

### Scope entities to discover processing activities with personal information

Determine which entities have and process personal information using the ServiceNow® Configuration Management Database (CMDB) application.

#### Before you begin

Ensure that you created the CMDB queries. For more information on the CMDB queries, see Querying the CMDB.

Role required: sn_privacy.manager

#### About this task

In the Configuration Management Database (CMDB), you can search the database for entities that process personal data using one of the following methods:

- Using the predefined queries and selecting only those applications and processes that have associated information objects. For more information about information objects and their role in Privacy Management, see Information objects in Privacy Management. For information on how to scope entities with personal information, see Scope entities to discover processing activities with personal information
- Building your own query. For more information on building the CMDB queries, see Querying the CMDB

To filter entities that contain personal data, you must filter the entities using the appropriate queries. ServiceNow® provides two default queries for you to use to filter entities with personal data. The default queries are provided for the following tables:

- Business process
- Business application

You can also create your own queries. This procedure demonstrates using the default queries.

#### Procedure

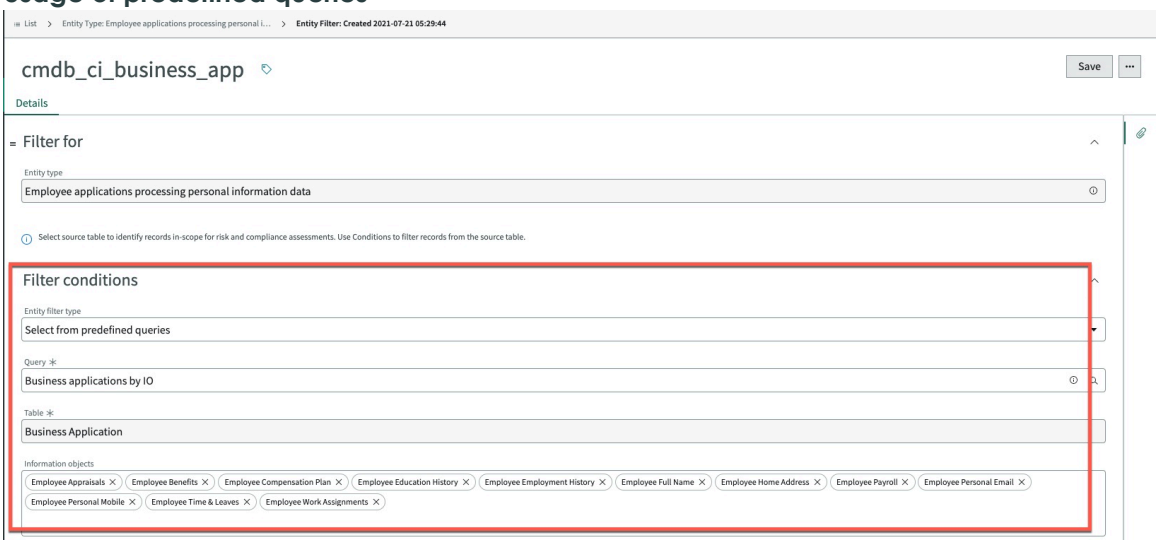
1. Navigate to **All** > **Privacy Workspace** > **Scoping** > **Entity types**.
2. Open the entity you want to filter for personal information.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click the Entity Filters related list.
4. Click **New**.
   The Entity Filter form is displayed.
5. In the Filter conditions section, in the **Entity filter type** field, select **Select from predefined queries**.
6. In the Query field, select **Business applications by IO**.
   The **Table** field is automatically set.
7. Optional: To add more information objects that contain personal information such as email address, click **Information objects** and type `Email`.
8. Click **Submit**.

**Example:**

**Usage of predefined queries**




## Types of privacy assessments

Privacy assessments can be sent using various methods such as entities, entity types, and processing activities.

Multiple types of privacy assessments such as privacy screening assessment, privacy impact assessment, transfer impact assessment, and so on can be configured according to your requirements.

### Initiating privacy assessments for an entity or a processing activity

To discover whether a business process or an application is processing personal data, you can use privacy screening assessments. To regularly assess how processing activities are processing personal data, you can use privacy assessments such as privacy impact assessment (PIA).

## Privacy screening assessment

Conducting a privacy screening assessment helps you discover whether the entity is processing personal information or not.

You can send the privacy screening assessments in the following ways:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- From the entity record only when a processing activity is not available.
- From the entities related list in entity types.

When you initiate privacy screening assessments for entities, processing activities are created based on the responses submitted by the entity owners.

**Note:** The processing activity creation rules can be configured based on the screening assessment responses.

After a processing activity is created, based on the assessment configurations, the following events occur:

1. The necessary information objects are mapped to the processing activity record. To understand more about information objects and their uses, see Information objects.
2. The necessary controls are mapped to the processing activity record.
3. Critical assessment responses such as the purpose of the processing activity, data subject type and so on are copied over to the processing activity record.

**Note:** If you accidentally send an assessment and the assessment is not completed, you can cancel the assessment.

## Privacy assessments

When processing activity records are identified, to understand how a processing activity is processing personal information, various types of privacy assessments such as privacy impact assessments (PIA) and transfer impact assessment (TIA) are sent. You can trigger PIAs from a single processing activity record. For more information, see Send a privacy assessment from a processing activity. Alternatively, you can send privacy impact assessments to multiple processing activities, using the Entity type capability or from the processing activity list view. For more information on how to send an assessment to multiple entities, see Send a privacy assessment to multiple entities.

Related topics

Send a privacy assessment to multiple entities

### Send a privacy assessment from an entity

Send a privacy assessment to an entity owner to determine if there's personal data involved in the processing activities.

#### Before you begin

Role required: sn_privacy.manager or sn_privacy.analyst

#### About this task

You can send a privacy screening assessment from an entity if you do not have a processing activity created for that entity. After a processing activity is created for an entity, any further assessments can only be sent through the processing activity.

#### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace** > **Scoping** > **My entities**.
2. Select and open the entity from which you want to send the assessments to the entity owner.
3. Select **Initiate privacy assessments**.
   You are redirected to the **Create new privacy assessment** form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. On the form, fill in the fields.
   For an explanation of the fields, refer to the New privacy assessment creation form
5. Select **Update state**.
   a. In the **State** field, select **Assigned**.
   b. In the **Additional comments** field, provide comments for the person taking the assessment.
   c. Select **Submit**.

### New privacy assessment creation form

Use the fields on the new privacy assessment creation form to create a new privacy assessment.

## Create a new privacy assessment creation form fields

**New privacy assessment creation form**

| Field | Description |
|---|---|
| Privacy assessment | |
| Number | Privacy assessment number. This field is automatically set. |
| Title | Name of the privacy assessment. |
| Requester | Name of the person requesting the assessment. |
| Assessment template | Template to be used for the assessment. |
| State | State of the assessment. This field is automatically set to **Draft**. |
| Priority | Priority of the assessment. |
| Description | Description of the assessment. |
| Assignment | |
| Assignee | Name of the person who will take the assignment. |
| Reviewers | Names of the persons who will review the assessment. You can select multiple reviewers in this field. |
| Schedule | |
| Due date | Date by which the assessment would be completed. |
| Accepted date | Date the assessment is accepted. This field is read-only and displays the date only when the task is accepted. |
| Created | Date the assessment is created. This field is read-only. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New privacy assessment creation form (continued)**

| Field | Description |
|---|---|
| Task closure date | Date when the assessment task is closed. This field is read-only and displays the date only when the task is closed. |
| Summary | |
| Observations | Observations about the assessment. |
| Activity | |
| Work notes (Private) | Work notes for the assessment. |
| Additional comments (Customer visible) | Comments for updating this assessment. |

### Send a privacy assessment to multiple entities

Send the privacy screening assessment or the Privacy impact assessment (PIA) assessments to multiple entities to understand why and how personal data is being processed.

#### Before you begin

Role required: sn_privacy.manager

#### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace** > **List** > **Scoping** > **Entity types**.
2. Select the entity types that contain the entities for which you want to send the assessments.
3. Select the entities related list.
4. To select the required entities, select the selection icon (☐).
5. Click **Send privacy assessments**.
6. From the **Classification** field, select the type of assessment.
7. From the **Assessment template** field, select the template you want to use.
8. In the **Due Date** field, select the due date for completing the assessment.
9. Click **Send**.

#### Result

The assessment is sent to the entity owners.

### Send a privacy assessment from a processing activity

Send a privacy assessment to a processing activity owner from a processing activity record to collect more information on why and how the processing activity is using personal information.

#### Before you begin

Role required: sn_privacy.manager or sn_privacy.analyst

#### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace** > **Processing activities** > **All processing activities**.
2. Select and open the processing activity from which you want to send a privacy assessment.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click **Initiate privacy assessments**.
   You are redirected to the **Create new privacy assessment** form.
4. On the form, fill in the fields.
   For an explanation of the fields, refer to the New privacy assessment creation form
5. Select **Update state**.
   a. In the **State** field, select **Assigned**.
   b. In the **Additional comments** field, provide comments for the person taking the assessment.
   c. Select **Submit**.

### Result
The assessment is sent to the entity owner.

#### Send privacy assessments from multiple processing activities

Send multiple privacy assessments from multiple processing activities. This capability enables you to filter the processing activities by business units, locations, data subjects, and data types.

### Before you begin
Role required: sn_privacy.manager or sn_privacy.analyst

### Procedure
1. Navigate to **All** > **Privacy Management** > **Privacy Workspace** > **Processing activities** > **All processing activities**.
2. Select the processing activities from which you want to send assessments.
3. Select **Send privacy assessments**.
4. From the **Classification** field, select the type of assessment.
5. From the **Assessment template** field, select the template you want to use.
6. In the **Due Date** field, select the due date for completing the assessment.
7. Click **Send**.

## Respond to a privacy assessment

As an entity owner or a processing activity key stakeholder, respond to the privacy assessment that is initiated by the privacy lead.

### Before you begin
Role required: sn_privacy.assessment_responder, sn_privacy.business_user

### About this task
While responding to an assessment, you can reassign the assessment to another user even if you have started the assessment. When you reassign the partially completed privacy assessment to another user, the data that is already provided also gets copied over and is available when the new assignee takes the assessment. This data can be modified by the new assignee.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Self Service** > **Employee Center** > **My active items** > **GRC tasks** > **My to-dos**.
2. Open the assessment assigned to you.
3. Perform one of the following actions.

| Choice | Action |
|---|---|
| To take the assessment | **a.** Select **Accept work**.<br>**Note:** Accepting the work creates an assessment instance.<br>**b.** In the Confirmation dialog box, provide your comments for the assessment.<br>**c.** Select **Accept work**.<br>**Note:** The privacy assessment moves to **Work in progress**.<br>**d.** Select **Take assessment**.<br>**e.** Respond to the questionnaire.<br>**f.** Select **Submit**. |
| To reassign the assessment | **a.** Select **Reassign**.<br>**b.** In the Reassign privacy assessment dialogue box, select an assignee.<br>**c.** In the **Additional comments** field, provide the reason for reassignment.<br>**d.** Select **Reassign**. |

### Result
The responses are captured in the respective entity and the processing activity. The responses are then reviewed by the privacy teams.

## Review a privacy assessment

As a privacy analyst, review a privacy assessment after the responders submit the assessment. You can either close the assessment after a review or you can also request for revision if you determine that the assessment requires more information.

### Before you begin
Role required: sn_privacy.analyst

### About this task
As a reviewer, you can also preview the assessment with the applicable risk statements, information objects, and control objectives.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Privacy Workspace** > **Tasks**.
2. Select and open the privacy assessment that you want to review.
3. Select **View response**.
4. Review the assessment responses.
5. To request for more information from the responder, select **Request for revision**.
6. To mark the assessment as complete, select **Update state**.
   a. In the **State** field, select **Closed complete**.
   b. In the Additional comments field, provide any additional information.
   c. Select **Submit**.

## Create or update a processing activity

Manually create a processing activity or update a processing activity that is automatically created out of a privacy screening assessment. You can also update a processing activity that is created from an entity record. When you update a processing activity, you can fill in the relevant details about the personal data that is being processed.

### Before you begin

Role required: sn_privacy.analyst (who owns the processing activity) or sn_privacy.manager

### Procedure

1. Navigate to one of the following.

| Action | Procedure |
|---|---|
| To create a new processing activity | a. Navigate to **All** > **Privacy Management** > **Processing activities** > **All processing activities**.<br>b. Click **New**. |
| To update a processing activity | a. Navigate to **All** > **Privacy Management** > **Privacy Workspace** > **List** > **My items** > **Processing activities**.<br>b. Open the processing activity that you want to update. |

2. On the form, fill in the fields.

#### New processing activity form

| Field | Description |
|---|---|
| Name | Name of the processing activity. |
| Processing activity purpose | Business justification or reason for using an application or a process that stores personal data. |
| Number | Number of the processing activity. This field is automatically set. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Privacy analyst | Analyst responsible for the processing activity. |
| Business unit | Business unit of the processing activity. |
| Department | Department of the processing activity. |
| Processing activity type | Context of the processing activity such as a business application or a business process. |
| Entity | Entity of the processing activity. |
| Applies to record | Reference record used to create the processing activity record. |
| Owned by | Owner of the processing activity. |
| Data processing role | Defines if a processing activity is a data controller or a data processor. |
| Processing activity status | Status of the processing activity. The choices are as follows:<br>◦ **Implementing**<br>◦ **In Production**<br>◦ **Pilot**<br>◦ **Retired**<br>◦ **Under Evaluation** |
| Processing activity category | Category to which the processing activity belongs for example, customer care, finance, and so on. |
| Compliance score | Privacy compliance score calculated based on all the controls mapped to this processing activity. |
| Process owner | Any user, with the sn_privacy.business_user role, from the list of key stakeholders who has the editing privileges for the processing activity.<br>**Note:** The user selected in this field can update the this field and select a new process owner. Updating this field is only possible when the processing activity is in the **Discover** or **Review** state. |
| Data subject | |
| Data storage type | Format in which the personal information is stored. The choices are as follows:<br>◦ **Digital**<br>◦ **Paper**<br>◦ **Both** |
| Data storage locations | Physical location of where the personal information is stored. |
| Data retention | Number of days for which personal information must be retained. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| period (in days) | |
| Data subject type | User type related to the personal information that is being used and processed. The choices are as follows:<br>◦ **Customers**<br>◦ **Employees**<br>◦ **Others** |
| Data subject range | Range of users for whom the personal information is being processed. |
| Contains special category data? | This field is automatically set to either **Yes** or **No**. If any information object associated with the processing activity is classified as special category data, then this field is automatically set to **Yes**. |
| Obtain special category data? | Does this processing activity process any special category data such as racial, ethnic, political information? The choices are as follows:<br>◦ **Yes**<br>◦ **No** |
| Activity | |
| Additional comments | Additional information about the processing activity. |
| Work notes | Internal notes not visible to the external people. |

3. Click **Save**.

## Create or manage an information object on a processing activity

Add information objects to the processing activity after a processing activity is created. Adding information objects helps you understand the types of personal information that is being processed and the way it is processed. This task helps in applying the appropriate controls to the processing activity.

### Before you begin

Role required: sn_privacy.analyst (who owns the processing activity) or sn_privacy.manager

### About this task

It is important to note that only the information objects that are tagged with the **Personal information** tags are available to be added to a processing activity. For more information on how to tag information objects see, Tag an information object with personal information.

### Procedure

1. Navigate to **All** > **Privacy Workspace** > **Processing activities** > **All processing activities**.
2. Select and open the processing activity to which you want to add controls.
3. Click the [PI] Information objects related list.
4. Click **Add**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Select the information objects you want to add.
6. Click **Add**.

Related topics

Modify an information object on a processing activity

### Modify an information object on a processing activity

Add details such as justification for storing data to an information object after you add it to the processing activity. Adding details enables you to define how the personal data is being processed.

#### Before you begin

Role required: sn_privacy.analyst (who owns the processing activity) or sn_privacy.manager

#### About this task

As a privacy analyst, you must provide details how personal data is being used in a given processing activity. Adding relevant details to an information object helps you achieve this objective.

#### Procedure

1. Navigate to **All** > **Privacy Workspace** > **Processing activities** > **All processing activities**.
2. Select and open the processing activity that contains the information object you want to modify.
3. Click the [PI] Information objects related list.
4. Open the information object that you want to modify.
5. On the Information object to processing activity form, fill in the fields.

| Field | Description |
|---|---|
| Information object | Name of the information object. This field is automatically set. |
| Processing activity | Name of the processing activity the information object is part of. This field is automatically set. |
| Data classification | Category of the data class. For example, **Highly Sensitive**. This field is automatically set. This field is defined when you set up the information object library. |
| Type of data | Type of personal data. The choices are the following:<br>◦ **General personal information**: Examples are: Name, phone number, address.<br>◦ **Special Category**: Examples are: Political opinions, religious beliefs, and so on. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** If any information object associated to a processing activity is categorized as Special category, the **Contains special category data?** field on the processing activity form is automatically set to **Yes**.<br>◦ **Criminal Conviction**: Examples are court verdicts, information about legal proceedings and so on. |
| Lawful basis for processing | Reason for processing personal data.<br>◦ **None**<br>◦ **Legal Obligation**<br>◦ **Legitimate Interests** |
| CRUD operations | Operations that can be performed on the processing activity. The choices are the following:<br>◦ **Create**<br>◦ **Read**<br>◦ **Update**<br>◦ **Delete** |
| Upstream processing activity | Source of inheriting data in the processing activity. For example, you can select the application from where the data in this processing activity is populated. |
| Downstream processing activity | Specify where the data is sent. |
| Justification for storing this data | Reasons for storing and using the personal data. |

6. Click **Save**.

## Add key stakeholders and send privacy assessments

Add key stakeholders to a processing activity to identify the key members who are responsible for processing the personal data within the processing activity. You can then send the respective privacy assessments to the stakeholders based on their responsibilities. For example, an entity owner is a key stakeholder for a processing activity.

### Before you begin

Role required: sn_privacy.analyst

### About this task

A processing activity can have multiple key stakeholders. While you can add or delete as many key stakeholders as you want, by default, the entity owner is one of the key stakeholders. All the stakeholders can respond to privacy assessments and some stakeholders can also edit the processing activity based on their privileges. Only users with the sn_privacy.assessment_responder and sn_privacy.business_user can be added as

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

stakeholders. You can add key stakeholders only when the processing activity is either in the **Discover** or **Review** states.

### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace** > **Processing activities** > **All processing activities**.
2. Open the processing activity to which you want to add key stakeholders.
3. Click the Key stakeholders related list.
4. Click **Add**.
   a. Select the stakeholders to add.
   b. Click **Add**.
      The key stakeholders are added.
5. To modify the privileges and responsibilities of a stakeholder, select the name of the stakeholder.
6. In the **Responsibility** field, provide the responsibilities of the stakeholder.
7. In the **Processing activity privileges** field, select one of the following options.

| Option | Result |
|---|---|
| Respond to privacy assessments | To enable the stakeholder only to respond to the privacy assessment.<br>**Note:** When you choose this option, the role of the stakeholder changes to sn_privacy.assessment_responder |
| Edit processing activity and respond to privacy assessments | To enable the stakeholder to edit and then respond to the privacy assessment.<br>**Note:** When you choose this option, the role of the stakeholder changes to sn_privacy.business_user |

8. Click **Save**.
9. Return to the processing activity using the breadcrumb navigation.
10. To send the privacy assessments to a stakeholder, click **Send privacy assessment**
    a. From the **Classification** field, select the type of assessment.
    b. From the **Assessment template** field, select the template you want to use.
    c. From the **User** field, select the user you want to send the assessment to.
    d. Click **Send**.

## Create or manage a control on a processing activity

Add new controls or manage the controls that are automatically added to the processing activity from the assessment responses. Adding controls ensures that the appropriate regulations are applied to the processing activity.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin

Role required: sn_privacy.analyst who owns the processing activity or sn_privacy.manager

### About this task

You can add or manage controls to a processing activity in the following ways:

- Selecting control objectives: You can add existing control objectives to a processing activity. When you add a control objective to a processing activity, the controls associated with that particular control objective are added to the processing activity.
- Creating controls: You can create controls and add them to the processing activity.
- Selecting from the recommended controls: This option enables you to choose from a list of recommended controls based on the information object that is mapped to a processing activity. If an information object is mapped to one or more control objectives, and the same information object is mapped to a processing activity, the system recommends the corresponding control objectives.
- Managing the automatically added controls: You can manage the controls that are automatically created based on the assessment responses.
- Applying controls from entities: You can apply privacy-related controls on the processing activity from the related entity.
- Adding common controls: You can add common controls to a processing activity so that the privacy teams can be notified of control failures and avoid duplicate common control attestation process. For more information on common controls, refer to Testing common control and implementing results on multiple reliant entities.

### Note:

### Procedure

1. Navigate to **All** > **Privacy Workspace** > **Processing activities** > **All processing activities**.
2. Select and open the processing activity to which you want to add controls.
3. Click the Controls related list.
4. To add a control to the processing activity, do one of the following.

| Option | Description |
|---|---|
| To create a control | Click **New** and fill in the form.<br>For details see, Create a control. |
| To add a control by using the existing control objectives | **a.** Click **Add controls by control objective**.<br>**b.** Select the control objectives that you want to add.<br>**c.** Click **Add**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| To select a control from the list of recommended controls | **a.** From the **Add controls by control objective** list, select **Recommend controls**.<br>**b.** Click **Add**.<br>**Note:** If a control has already been added to a processing activity, then it does not appear in the list of recommendations. |

**Result**
The mitigating controls are added to the processing activity.

## Delete a control from a processing activity

Delete the controls that are no longer required in the processing activity.

**Before you begin**
Role required: sn_privacy.admin

**About this task**
You can delete controls if the control objectives associated with those controls have been erroneously added. If you want to add new controls, you may want to delete existing controls.

**Note:** If a control is associated with any other entity or entity type, then you cannot delete the control. By deleting a control, you can only remove the association of that control with the processing activity.

**Procedure**

1. Navigate to **All** > **Privacy Workspace** > **Processing activities** > **All processing activities**.
2. Select and open the processing activity from which you want to delete controls.
3. Click the Controls related list.
4. Select the controls that you want to delete.
5. Click **Delete**.

**Result**
The selected controls are deleted from the processing activity.

## Create or manage risks on a processing activity

Add new risks or manage the risks that are automatically added to the processing activity from the assessment responses. Adding risks helps you manage processing activities using the risk-based approach.

**Before you begin**
Role required: sn_privacy.analyst who owns the processing activity or sn_privacy.manager

**About this task**
You can add or manage risks to a processing activity in the following ways:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Selecting risk statements: You can add existing risk statements to a processing activity. When you add a risk statements to a processing activity, the risks associated with that particular risk statement are added to the processing activity.
- Selecting from the recommended risks: This option enables you to choose from a list of recommended risks based on the information object that is mapped to a processing activity. If an information object is mapped to one or more risk statements, and the same information object is mapped to a processing activity, the system recommends the corresponding risk statements.
- Creating risks: You can create risks and add them to the processing activity.
- Applying risks from entities: You can apply privacy-related risks on the processing activity from the related entity.

### Procedure

1. Navigate to **All** > **Privacy Workspace** > **Processing activities** > **All processing activities**.
2. Select and open the processing activity to which you want to add controls.
3. Click the Risks related list.
4. To add a risk to the processing activity, do one of the following.

| Option | Description |
|---|---|
| To create a risk | Click **New** and fill in the form.<br>For details see, Create a risk. |
| To add a risk by using the existing risk statement | **a.** Click **Add risk by risk statement**.<br>**b.** Select the risk statements that you want to add.<br>**c.** Click **Add**. |
| To select a risk from the list of recommended risks | **a.** From the **Add risk by risk statement** list, select **Recommend risks**.<br>**b.** Click **Add**.<br>**Note:** If a risk has already been added to a processing activity, then it does not appear in the list of recommendations. |

### Result

The mitigating controls are added to the processing activity.

## Create or add issues on a processing activity

Create issues or add existing issues for a processing activity. Associating issues to a processing activity helps you to identify and prioritize remediation actions. Relating issues reduces the number of issues customers need to manage, thus improving the overall organizational efficiency in management of these issues.

### Before you begin

Role required: sn_privacy.analyst (who owns the processing activity) or sn_privacy.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task
Issues get created when there are control attestation failures. You can also manually add or create multiple issues for a processing activity. You can also map one issue to multiple processing activities. If you create an issue for a processing activity from the Privacy Workspace, the **Issue source** field is set to **Ad-Hoc**.

### Procedure
1. Navigate to **All** > **Privacy Workspace** > **Processing activities** > **All processing activities**.
2. Select and open the processing activity to which you want to add issues.
3. Click the More related list.
4. Click Issues.
5. Click **Add**.
   a. Select the issues to add.
   b. Click**Add**.
6. Optional:  To create an issue, refer to the issue creation form.
7. Click **Save**.

## Assign a processing activity to a key stakeholder

Assign a processing activity to the defined key stakeholders for the stakeholders to start working on the processing activity.

### Before you begin
Role required: sn_privacy.analyst

### About this task
You can assign a processing activity to a key stakeholder when the processing activity is in the **Discover** state. After the key stakeholder updates the processing activity, they can assign the processing activity back to the privacy team.

### Procedure
1. Navigate to **All** > **Privacy Management** > **Privacy Workspace** > **List** > **Processing activities** > **Unassigned processing activities**.
2. Select the processing activity that you want to assign to a key stakeholder.
3. Select **Assign to key stakeholder**.
4. In the Assign to key stakeholder window, select a stakeholder.
5. Select **Assign**.

### Result
The processing activity is assigned to the key stakeholder. The processing activity is available for review and update in the Employee Center under **GRC tasks**.

Related topics

Integrating Employee Center and Risk portal with Privacy Management

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Integrating Employee Center and Risk portal with Privacy Management

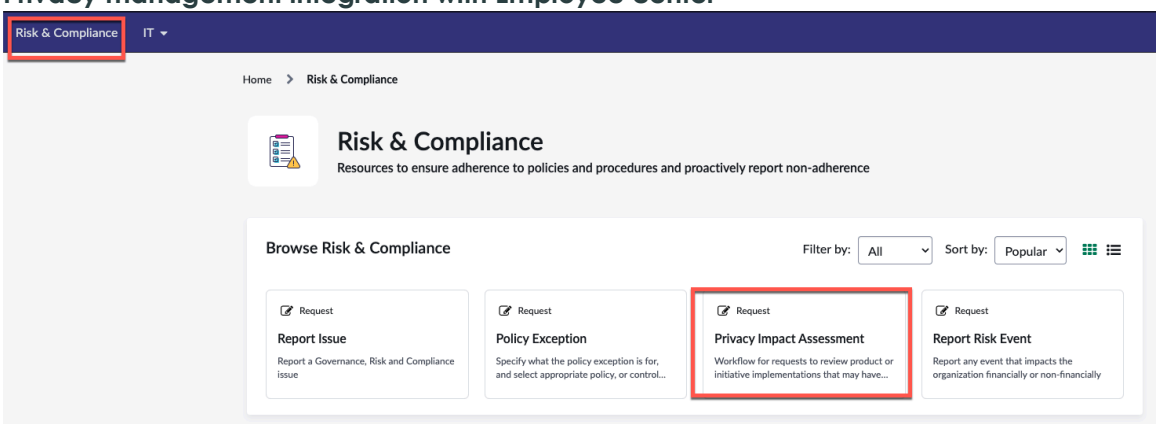
The integration of Employee Center with Privacy Management provides all employees and users a simplified user experience to perform tasks such as submitting a privacy impact assessment for a new implementation, responding to control attestations, and accessing processing activities and privacy impact assessments.

## Employee Center

The Employee Center portal is a unified portal that helps connect systems across the enterprise to one destination site that provides a simple and centralized experience for employees with easy to configure options. To learn more about the Employee Center, refer to Exploring Employee Center.

If you integrate Privacy Management with the Employee Center, you can provide all employees an interface to create a privacy impact assessment that would result in the creation of a processing activity. Only users with the roles sn_privacy.assessment_responder and sn_privacy.business_user can view the option to create a privacy impact assessment. The following image shows the page from where you can submit a new implementation request. For example, a team can use the Employee Center if a business plans a new implementation. Before creating a business application record, the team can contact the privacy team by responding to the Privacy Impact Assessment for the new implementation request. This helps to get the privacy team's guidance in the initial or inception phase of the new implementation.

**Privacy management integration with Employee center**

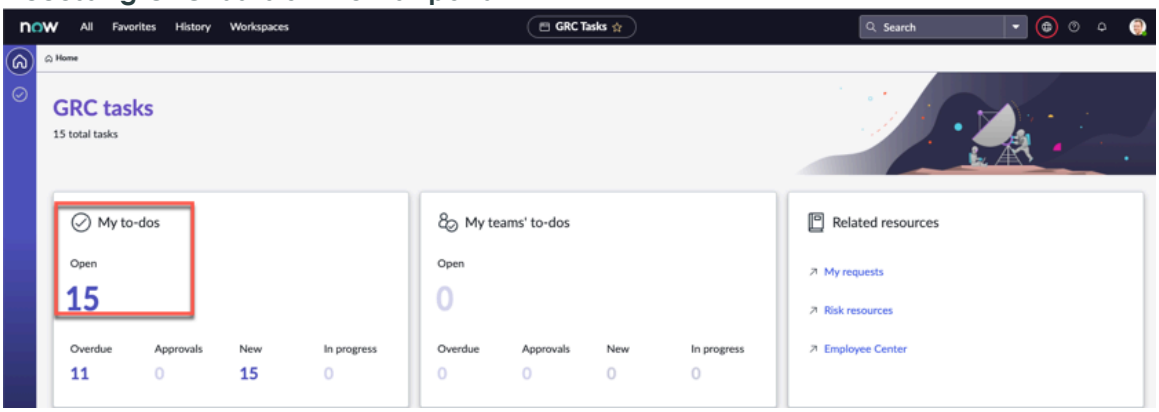



## Risk portal

If a privacy analyst assigns a processing activity to a business user to get more details on the processing activity, the business users can access the assigned processing activity from the risk portal.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Accessing GRC tasks on the Risk portal




## Privacy Case Management

The Governance, Risk, and Compliance: Privacy Case Management application enables you to report and manage privacy violations and complaints. The solution allows for the swift and efficient management of privacy breaches and complaints through collaboration with various teams which help in investigating the root cause and key details of the breach reported.

With the ability to integrate with other systems and record impacted areas, the application helps to identify key stakeholders and information objects associated with a case. This helps privacy teams to take appropriate preventive measures and remediation steps to manage the breach and its impact.

| Explore | Configure | Use |
|---|---|---|
| Learn about how privacy managers, privacy users, and privacy administrators use the Privacy Case Management application. | Configure your Privacy Case Management application. | Work on creating privacy assessments, processing activities and so on. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Reference | | |
|---|---|---|
|  Learn about the tables and roles that are installed with the Privacy Case Management application. | | |

## Exploring Privacy Case Management

The Governance, Risk, and Compliance: Privacy Case Management application enables users to report any privacy breaches or complaints, collaborate with key stakeholders, perform breach investigations, and analyse the causes and consequences of breaches.

Some examples of when privacy cases arise are as follows:

- Lost IT assets
- Exposed customer data
- An email delivered to a group of wrong recipients
- Loss of paperwork and documentation

The Privacy Case Management application helps the privacy teams to manage any case that involves a privacy violation or a breach. The privacy cases can be reported by any user using the Employee Center or can also be created by the privacy teams using the Privacy Workspace. The application facilitates APIs to create privacy cases from various sources such as other ServiceNow solutions, for example, Security Incident Response, IT Incidents, HR Cases, and third party integrations.

The Privacy Case Management application offers the following benefits for your organization:

- Helps business users to report any privacy breaches or complaints that require the attention of the privacy teams.
- Ensures collaboration with multiple teams to investigate, assess, gather evidence, capture observations, and responses for further review.
- Records the impacted areas and related areas that must be addressed such as policies and regulations, IT assets, impacted business units, and so on.
- Helps to identify key stakeholders and information objects associated with the case.
- Provides the ability to initiate remediation, preventive measures, and conduct root cause analysis to eradicate the cause of the case.
- Helps to identify and manage issues that arise from the privacy cases.

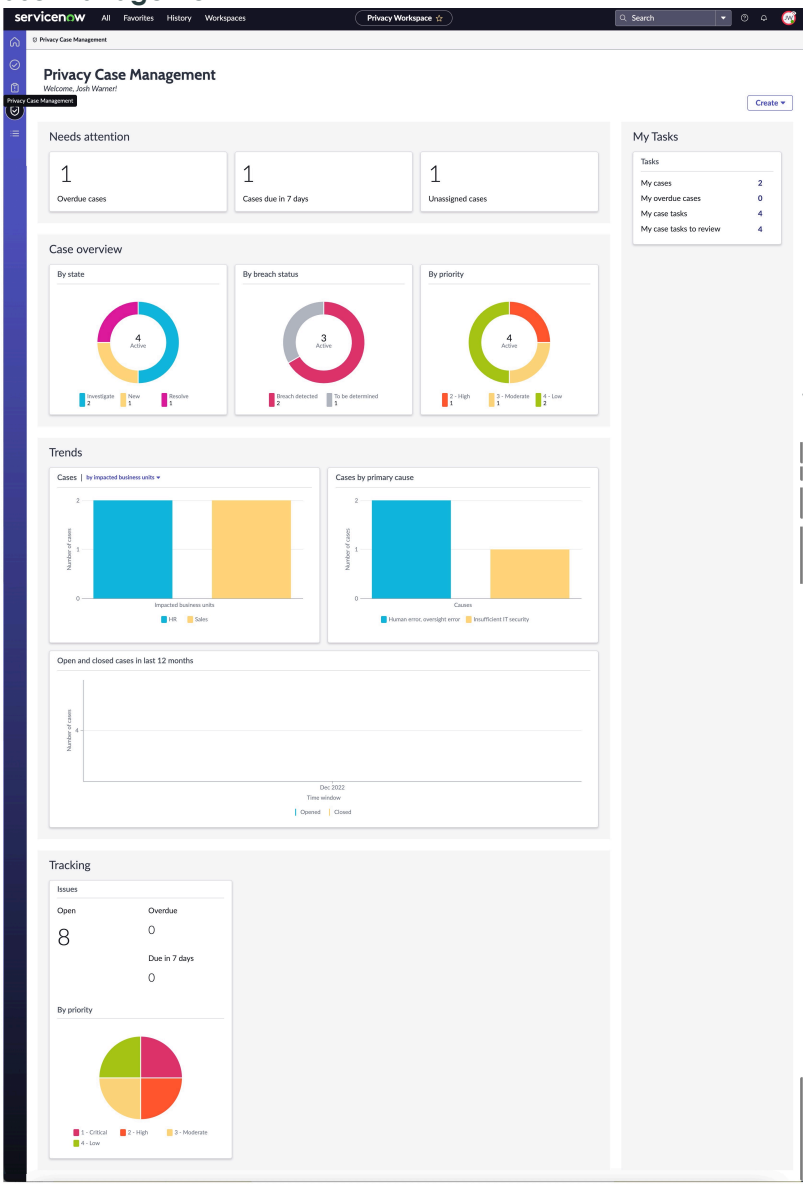
### Privacy Case Management home page

The Privacy Case Management application home page offers the privacy case manager an overview of all your privacy case-related information such as cases that need immediate attention, graphical dashboards to view cases by status, breach status, priority, and so on.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The privacy manager has the role sn_privacy_case.privacy_case_manager, and can launch the Privacy Case Management landing page using the launcher ( ) icon from the Privacy Workspace. The landing page shows the privacy managers the cases and case tasks assigned to them and also the cases that are overdue.

### Landing page for Privacy Case Management




The Privacy Case Management landing page displays the following sections for the privacy case manager:

- Needs attention
- Case overview
- Trends
- Tracking
- My tasks

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Needs attention

The **Needs attention** section gives you an overview of the events or cases that need immediate attention. This section includes the following information:

- **Overdue cases**: Cases for which the closure date has passed.
- **Cases due in 7 days**: Cases for which the closure date is in the next seven days.
- **Unassigned cases**: Cases not yet assigned to a case analyst.

## Case overview

The **Case overview** section gives you a graphical representation of all the active cases based on state, breach status, and priority.

- **By state**: Displays the number of active cases based on the workflow states that they are in. For example, as a privacy case manager you can view the number of active cases that are under the investigation state. The states displayed are as follows:
  - **New**
  - **Triage**
  - **Investigate**
  - **Resolve**
  - **Post case review**
- **By breach status**: Displays the number of active cases by the status that are as follows:
  - **Breach detected**
  - **To be determined**
  - **Future potential**
- **By priority**: Displays the number of active cases based on the priority defined at the case level. The priorities are as follows:
  - **High**
  - **Moderate**
  - **Low**
  - **Critical**
  - **Planning**

## Trends

The **Trends** section helps you to visualize the following:

- Number of reported privacy breaches and complaints based on the affected business units and geographical locations.
- Number of privacy cases reported for each primary cause.
- Number of privacy violation and complaint cases open and closed in the last 365 days.
- Cases by impacted business units and by locations.
- Cases by their primary causes
- Open and closed cases in the last 12 months.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Tracking

The **Tracking** section displays the following:

- Number of open issues for a privacy case.
- Number of overdue issues.
- Number of issues due in the next seven days.

**Note:** The privacy teams can also create privacy cases and privacy-related issues from the landing page.

## My tasks

The **My tasks** section helps you to access all the cases and tasks that have been assigned to you. This section includes the following information:

- **Cases**: All the cases assigned to you.
- **Overdue cases**: Any overdue cases with you.
- **Case tasks**: All the case tasks assigned to you to work on.
- **Case tasks to review**: Case tasks pending with you to review. For example, as a case analyst you've created a case task and assigned it to a case task owner to work on it. The case task owner completed the case task and submitted it to you for review. All such cases are available in this section.

### Privacy Case overview page

The Privacy case overview page shows details, such as description, state, schedule and milestones, case tasks, and issues related to the case in the Privacy Case Management application.

The Privacy Case Management overview related list includes the following sections:

- Description
- State
- Case schedules and milestones
- Case tasks overview
- Tracking
- Attachments

## Description section

The Description section includes the detailed information that you can fill in when you're creating a privacy case. For example, you can add the purpose, action being taken, time line, applicable rules and regulations, and any relevant evidence or documents. By using this section, you can understand the context of the case and take the necessary steps to resolve it.

## State section

The State section includes the workflow states of a privacy case. For example in this section, you see various stages of the privacy case, such as New, Triage, Investigate, Resolve, Post case review, and Close. These states determine the status of the case. A privacy case administrator can configure these states in the Privacy Case Management application. For more information, see Define the workflow states for a privacy case.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Case schedules and milestones section

The Case schedules and milestones section includes the details on all the milestones or events during the case life cycle in a time-line range. In this section, you can see an outline of the key events, such as the date when the case was reported, occurred, discovered, or closed. You can also filter the events to view the following options on the time-line range after you select the **Show events** option:

Case creation date
: Date when the case was created.

Date of discovery
: Date when the case was discovered.

Date of occurrence
: Date when the case occurred.

Milestone
: Dates related to the investigation remediation milestones.

Breach
: Dates related to the breach analysis.

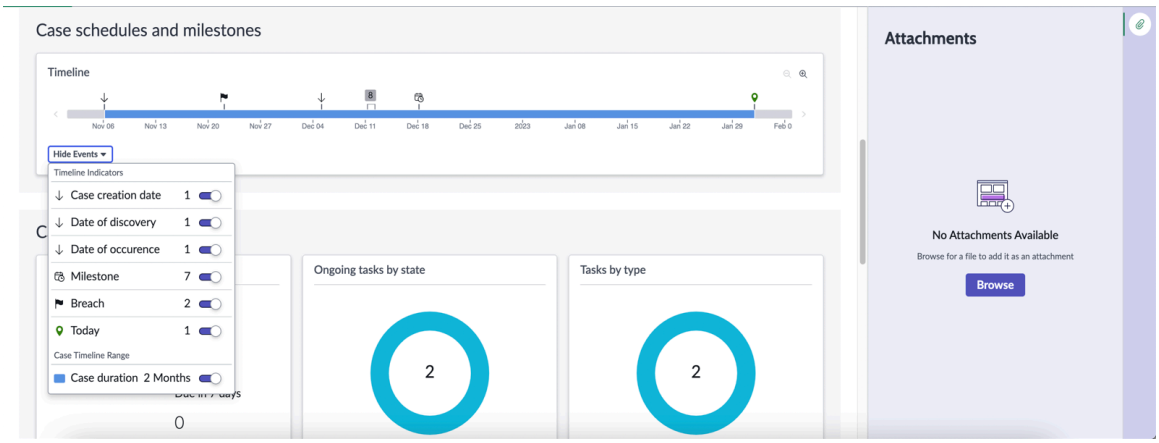
Today
: Current date on the time line.

Case closure
: Date when the case was closed or met the case closure service level agreement (SLA).

Case duration
: Date when the case was created to the last milestone date.

The following example shows the options available after you select the **Show events** option.

### Case schedules milestones




**Note:** The options that are displayed after you select the **Show events** option are limited to the events and milestones that are available for the case.

## Case tasks overview section

The case task overview section includes the following subsections:

Tasks

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Total number of case tasks, any overdue case tasks, and case tasks that are due in seven days.

Ongoing tasks by state

Number of active case tasks by the states.

Tasks by type

Number of active case tasks by the case type.

## Tracking section

The Tracking section displays the following information:

- Number of open issues for a privacy case
- Number of overdue issues
- Number of issues due in the next seven days

## Attachments section

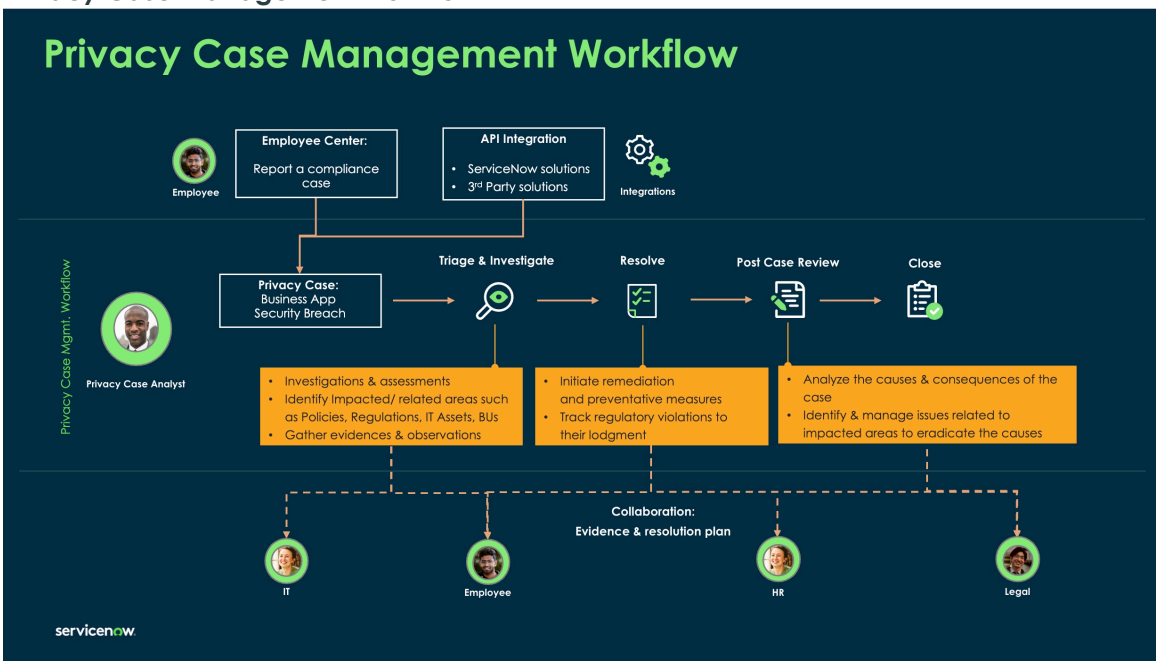
The Attachment section enables you to upload a file as an attachment to a case. In this section you can find all the attachments that have been added.

### Privacy Case Management workflow

The Privacy Case Management solution provides you a framework to manage any privacy breaches reported by the users. The solution provides an end-to-end workflow for the privacy team to triage the reported breach and perform the required investigation and analysis, gather evidence, record the key stakeholders, impacted areas, and regulatory violations, if any.

The following image shows the workflow of the Privacy Case Management application.

**Privacy Case Management workflow**




The life cycle of a privacy case is explained as follows:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. A case can be reported by the business users from the Employee Center or users can also reach out to the privacy teams using other modes such as phone call or email, after which the privacy team can create the case on behalf of the user from the Privacy Workspace and attach the related details.
2. The privacy case team assigns a case analyst to the case.
3. The case analyst triages and investigates the case and creates Case task workflow tasks. Each task is assigned to a case task owner.
4. The case task owners add the relevant details to the tasks and submit them for the case analyst to review.
5. The case analyst then does the following tasks:
   a. Reviews the responses submitted by the task owners.
   b. Records [PI] information objects, key stakeholders, impacted areas, and related areas.
   c. Tracks regulatory breaches and their appropriate lodgement.
   d. Initiates preventive measures and tracks the causes and their consequences.
   e. Manages the issues that arise out of the impacted areas.
6. The case analyst reviews all the details and closes the case.

### Privacy breach assessment

Privacy breach assessments play an important role whenever there is an incident that threatens the privacy of individuals. These assessments help to determine if there is a breach and then serve as a measure to gauge the extent and impact of a breach.

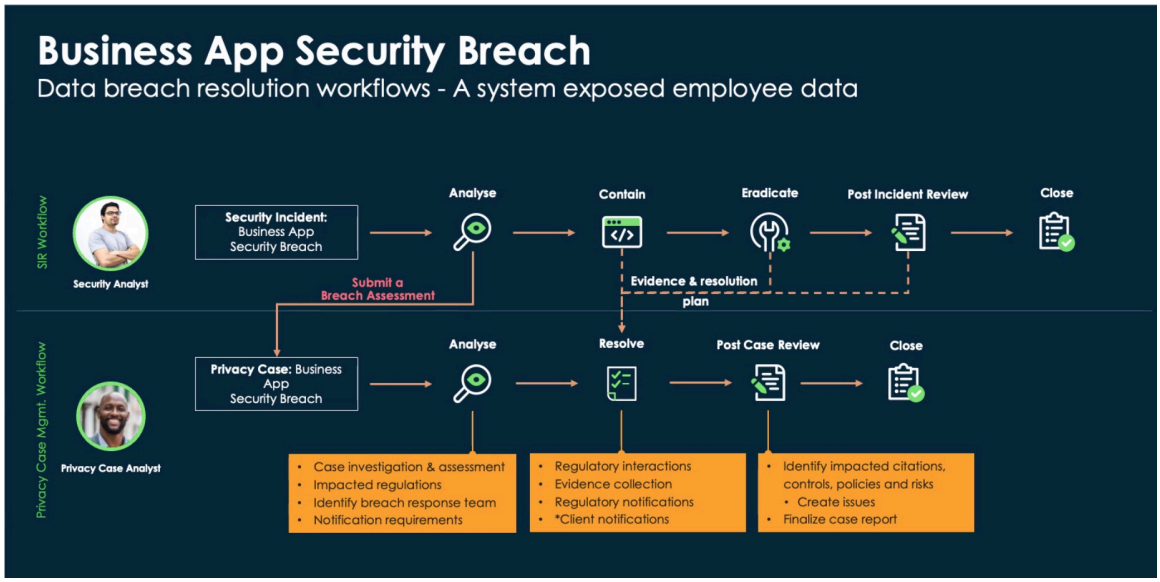
There are two pathways to trigger a breach assessment: it can be initiated directly from a privacy case or you can initiate the breach assessment as a standalone assessment. When an assessment is initiated as a standalone assessment, the results are analysed and a privacy case may be created if required. This flexibility ensures that organizations can promptly respond to potential breaches. You can perform only one breach assessment for each privacy case.

In the event of a breach, any specific criteria, for example, a server being compromised with personal data, may prompt the initiation of a breach assessment before creating a privacy case. The primary objective of this assessment is to quickly determine the nature of the compromised data. For example, if the incident is related to security incident, the security analysts are tasked with filling out the breach assessment, providing details on the incident type, impacted locations, and any existing mitigation measures like encryption. Subsequently, privacy analysts review the assessment, delving into the specifics of the incident. Based on this analysis, a privacy case may be created to prevent future occurrences and manage legal obligations linked to the breach.

The following image illustrates the breach assessment workflow using the example of a security incident.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Privacy breach assessment workflow




## Configuring Privacy Case Management

Follow the order of the tasks given here to configure Privacy Case Management application. These tasks help you to manage the compliance cases effectively.

### Install Privacy Case Management

You can install the Privacy Case Management application (sn_privacy_case) if you have the admin role.The application includes demo data and installs related ServiceNow® Store applications and plugins if they are not already installed.

### Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application .

Role required: admin

### About this task

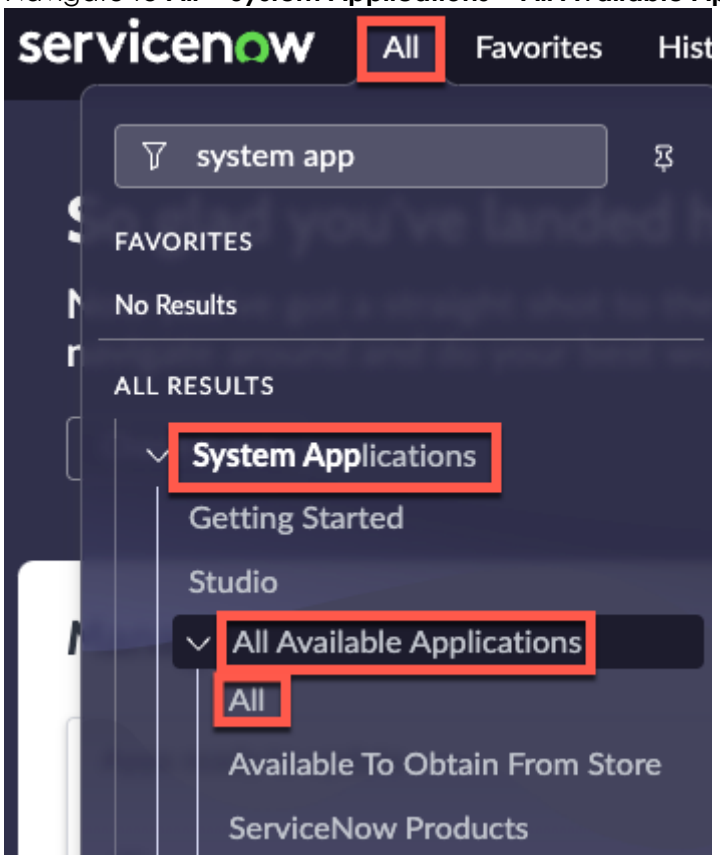
The following items are installed with Privacy Case Management:

- Plugins
- Store applications
- Roles
- Scheduled jobs
- Tables

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.




2. Find the Privacy Case Management application (sn_privacy_case) using the filter criteria and search bar.

   You can search for the application by its name or ID. If you cannot find the application, you might have to request it from the ServiceNow Store.

   In the list next to the **Install** button, the versions that are available to you are displayed.

3. Select a version from the list and select **Install**.

   In the Install dialog box that is displayed, any dependencies that are installed along with your application are listed.

4. If you are prompted, follow the links to the ServiceNow Store to get any additional entitlements for dependencies.
5. Optional: If demo data is available and you want to install it, select the **Load demo data** check box.
   Demo data comprises the sample records that describe application features for the common use cases. Load the demo data when you first install the application on a development or test instance.

   > **Important:** If you don't load the demo data during installation, it's unavailable to load later.

6. Select **Install**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create a view rule

Create view rules to define the form view of the privacy cases in the Privacy Workspace. Specifying the rules helps you to control how the privacy case form appears.

#### Before you begin

Role required: sn_privacy_case.privacy_case_admin

#### Procedure

1. Navigate to **All** > **Privacy Case Management** > **Case type**.
2. Select the **View Rules** related list on the case type form.
3. Select **New**.
4. On the View Rule form, fill in the fields.
   For a description of the fields on the View Rule form, see View rule form.
5. Select **Submit**.

### View rule form

Learn about the fields on the view rule form. Use this form to define workspace and default view rules in the Privacy Case Management application.

On the view rule form, fill in the fields.

**View rule form**

| Field | Description |
|---|---|
| Name | Unique name to identify the rule. |
| Table | Table this view rule applies to. This field is automatically set to **Privacy case [sn_privacy_case_privacy_case]**. |
| View | View for which you're creating the rule. The choices are as follows:<br>• **Default view**: Select this option to define the form view on the Core UI.<br>• **Workspace**: Select this option to define the form view on the Privacy Workspace. |
| Experience Restricted | Option to decide if the rule must be restricted to one workspace or to multiple workspaces. |
| Application | Name of the application this view rule applies to. This field is automatically set to **GRC: Advanced Risk**. |
| Execution Order | Order in which this view rule executes if there are multiple rules. |
| Active | Option to activate the view rule. |

### Create an assignment rule

Specify the conditions for assigning a privacy case to a particular user or group by creating assignment rules.

#### Before you begin

Role required: sn_privacy_case.privacy_case_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

To determine the appropriate person or group to handle a privacy case, establish assignment rules that outline the necessary criteria. For instance, if the case pertains to data protection and information security, it should be assigned to the appropriate individual or team.

### Procedure

1. Navigate to **All** > **Privacy Case Management** > **Case type**.
2. Select the **Assignment Rules** related list on the Assignment Rule form.
3. Select **New**.
4. On the Assignment Rule form, fill in the fields.
   For a description of the field values on the Assignment Rule form, see Assignment rule form.
5. Select **Submit**.

#### Assignment rule form

Learn about the fields on the assignment rule form. Use this form to define case assignment rules in the Privacy Case Management application.

## Assignment rule form

For a description of the field values, see the following table:

**Assignment rule form**

| Field | Description |
|---|---|
| Name | Name of the assignment rule. |
| Application | Name of the application this assignment rule applies to. This field is automatically set to **GRC: Privacy Case Management**. |
| Active | Option to enable the assignment rule. |
| Applies To | |
| Table | Table this assignment rule applies to. This field is automatically set to **Privacy case [sn_privacy_case_privacy_case]**. |
| Conditions | Conditions to be defined for the case type's assignment rule. |
| Assign to | |
| User | User the case is assigned to. |
| Group | Group the case is assigned to. |
| Script | |
| Script | Script to define advanced assignment rule. |

#### Create state model transition

Create state models to control the workflow of a privacy case by defining the states and transition conditions.

### Before you begin

Ensure that you are in the GRC: Privacy Case Management application.

Role required: sn_privacy_case.privacy_case_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Privacy Case Management** > **State Models**.
2. Select **New**.
3. On the form, fill in the fields.

**State model form**

| Field | Description |
|---|---|
| Name | Name of the state model. For example, `Breach case`. |
| Application | Scope of the application. This field is automatically set to **GRC: Privacy Case Management**. |
| Active | Option to indicate that the state model is active or inactive. |
| Table name | Table this state model applies to. |
| State model field | Fields that contain the state model value in the table that this state model applies to. |
| State field | Fields that contain the state value in the table that this state model applies to. This field is automatically set to **State [state]**. |

4. Select **Submit**.

## Define the workflow states for a privacy case

Define the workflow states for a privacy case that govern the lifecycle of the case.

### Before you begin

Role required: sn_privacy_case.privacy_case_admin

### About this task

A privacy case typically goes through the following workflow states that can be configured in the Privacy Case Management application:

- New: The case has been opened and is in the initial stage of review.
- Triage: The case is being evaluated to determine the appropriate course of action.
- Investigate: The case is being actively investigated to gather information and evidence.
- Resolve: The case is being worked on to find a resolution.
- Post case review: A review of the case is being done after it is resolved.
- Close: The case is closed and is no longer active.
- Cancel:The case is cancelled and it is no longer being pursued.

These states can vary depending on the organization's privacy case management process.

### Procedure

1. Navigate to **All** > **Privacy Case Management** > **State Models**.
2. Open the state model that you created and want to add the workflow for.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. On the GRC workflow states context menu, select **New**.
4. On the form, fill in the fields.

**Workflow state form**

| Field | Description |
|---|---|
| State | Name of the workflow state. Choices are the following:<br>◦ **New**<br>◦ **Triage**<br>◦ **Investigate**<br>◦ **Resolve**<br>◦ **Post case review**<br>◦ **Close**<br>◦ **Canceled** |
| Model | State model that uses this workflow state. This field is automatically set to the state model name. |
| Application | Name of the application this state model applies to. This field is automatically set to **GRC: Privacy Case Management**. |
| Display type | Display type of the workflow state. Choices are the following:<br>◦ **As node**: Display as a parent state.<br>◦ **As sub-level**: Display as a sub-state of the parent state. |
| Stepper label | Label to be displayed on the stepper component for the state. |
| Parent model state | Parent state for the sub-level state. This field appears only when **As sub-level** is selected from **Display type**. |
| Is optional | Option to select the state as optional. This field appears only when **As node** is selected from the **Display type** field. |

5. Create the other states similarly.
6. Select **Submit**.

### Define the model state transitions for a privacy case

Define the transition conditions to control how a compliance case traverses through the different workflow states by using the Privacy Case Management application.

**Before you begin**
Role required: sn_privacy_case.privacy_case_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

The state transitions are a list of conditions for entering or exiting each state that is defined for a table. In the State Transitions table, use the condition builder to build a list of required conditions for entering or exiting each state.

### Procedure

1. Navigate to **All** > **Privacy Case Management** > **State Models**.
2. Open the state model that you want to define the model state transition for.
3. To define the model state transition, select the required workflow state.
4. On the Model State Transitions context menu, select **New**.
5. Select the state that you want to move to from the selected state.
6. Optional: To enable the automatic transition of the workflow state, select the **Automatic transition** option.
7. Open the form context menu and select **Save**.
   The GRC model state transition conditions related list appears.
8. On the GRC model state transition conditions context menu, select **New**.
9. On the form, fill in the fields.

   For a description of the field values on the GRC model state transition form, see GRC model state transition condition form.
10. Select **Submit**.

#### GRC model state transition condition form

Use the GRC Model State Transition Condition form to define the transition conditions to control how a compliance case traverses through the different workflow states by using the Privacy Case Management application.

See the following table for a description of the field values.

##### GRC Model State Transition Condition

| Field | Description |
|---|---|
| Name | Name of the condition. |
| State transition | Transition of states. This field is automatically set to the model state transition value. |
| Active | Option to enable the model state transition condition. |
| Description | Description of this state transition. For example, in the **Description** field for the New state, you could enter `New state can move only to Analyze state`. |
| Error message | Error message to be displayed when the conditions aren't met. |
| Requires | Transition conditions: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**GRC Model State Transition Condition (continued)**

| Field | Description |
|---|---|
| | • **Task has been through Approval**: Condition passes if the related task has an approval that is either accepted or rejected.<br>• **Task is Approved**: Condition passes when the task is approved.<br>• **Task is Rejected**: Condition passes when the task is rejected.<br>• **Transition Condition**: Conditions for this state transition.<br>• **Transition Script**: Advanced conditions for this state transition. |
| Condition | Conditions to be defined for this state transition. This field appears only when **Transition Condition** is selected from **Requires**. |
| Script | Script to be defined for this state transition. This field appears only when **Transition Script** is selected from **Requires**. |

### Create a privacy case assessment template

Create an assessment and send those assessments to the privacy case task owners to collect their responses. The responses help the privacy case analysts to determine the breaches that have occurred due to the privacy case.

#### Before you begin
Role required: sn_privacy_case.privacy_case_admin

#### About this task
Instead of using the default template, you can create a questionnaire template for assessing privacy cases. After you set up the assessment template, it's available in the case task section for the **Assessment** case type.

#### Procedure
1. Navigate to **All** > **Privacy Case Management** > **Assessment Templates**.
2. Select **New**.
3. On the Assessment Metric Type form, fill in the fields.
   For a description of the field values on the Assessment Metric Type form, see Assessment metric type form.
4. Select **Submit**.

### Assessment metric type form

Use the Assessment Metric Type form to create an assessment questionnaire template instead of using the default template.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Assessment metric type form

For a description of the fields, see the following table:

**Assessment metric type form**

| Field | Description |
|---|---|
| Name | Name of the assessment template. |
| Assessment duration | Length of time allowed for completing the assessment from the time the assessment is generated. |
| Table | Table this assessment template applies to. |
| State | Status of the assessment. This field is automatically set to **Draft**. |
| Roles | Roles that have read access to the template. |
| Description | Purpose of the assessment template and the reason for its creation. |
| Introduction | Guidance text for business users who respond to the assessment. |

## Configuring privacy breach assessment

Follow the order of the steps such as creating breach factor types, breach factors, PI data element types, and PI data elements to configure privacy breach assessment.

### Create a breach factor type

Create categories to help responders to identify breach factors within specific categories. For example, incident nature is a breach factor type which has factors under it as Intentional and Malicious, or Intentional and not malicious, and Unintentional or inadvertent.

**Before you begin**
Role required: sn_privacy_case.privacy_case_admin

**Procedure**

1. Navigate to **All** > **Privacy Case Management** > **Breach Assessment Configuration** > **Breach Factor Types**.
2. Select **New**.
3. On the form, fill in the fields.

**Breach factor type form**

| Field | Description |
|---|---|
| Label | Category to which the factor type belongs. For example, Incident nature, Recipient and so on. |
| Name | Element of the breach factor. |
| Active | Option to activate the factor. |
| Application | Name of the application this factor applies to. This field is automatically set to **GRC: Privacy Case Management**. |
| Description | Brief description of the breach factor type. |

4. Select **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create breach factors

Create breach factors to help privacy teams understand the characteristics of a breach and evaluate the related risks. Exercise your flexibility to either use the default breach factors or generate new ones. Additionally, link breach factors to specific regions or implement them universally across multiple regions or selected ones.

#### Before you begin

Role required: sn_privacy_case.privacy_case_admin

#### Procedure

1. Navigate to **All** > **Privacy Case Management** > **Breach Assessment Configuration** > **Breach factor**.
2. On the form, fill in the fields.

**Breach factor form**

| Field | Description |
|---|---|
| Label | Category to which the factor belongs. For example, Electronic, Paper, and so on. |
| Name | Unique name to identify the factor. |
| Type | Type of preconfigured breach factors with which the factor must be associated. |
| Application | Name of the application this factor applies to. This field is automatically set to **GRC: Privacy Case Management**. |
| Active | Option to activate the factor. |
| Applied to | Location of where the factor is applicable. The options are as follows:<br>◦ **All regions**<br>◦ **Specific to a region** |
| Description | Brief description of the factor. |

3. Select **Submit**.

### Create a PI data element type

Create categories to help responders to identify personal data elements within specific categories. For example, for a PI data element type such as Personal information, the PI data elements can be Name, Age, Employer ID, Marital Status, Email, and so on.

#### Before you begin

Role required: sn_privacy_case.privacy_case_admin

#### Procedure

1. Navigate to **All** > **Privacy Case Management** > **Breach Assessment Configuration** > **PI Data Element Types**.
2. Select **New**.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

#### PI data elements type form

| Field | Description |
|---|---|
| Label | Category to which the PI data element type belongs. For example, for type `Financial Information`, the data elements can be bank account numbers, credit card numbers, and so on. |
| Name | Name of the PI data element type. This name is usually the same as the label. |
| Order | Order of the element type as it should appear on the assessment form. |
| Application | Name of the application this element type applies to. This field is automatically set to **GRC: Privacy Case Management**. |
| Active | Option to activate the data element type. |
| Description | Brief description of the PI data element type. |

4. Select **Submit**.

### Create PI data elements

Create PI data elements based on residents' personal information collected during the business process, such as phone numbers and email IDs. Use pre-configured elements or create new ones. Customize for data elements for specific regions or map a single PI data element to multiple regions.

## Before you begin

Role required: sn_privacy_case.privacy_case_admin

## Procedure

1. Navigate to **All** > **Privacy Case Management** > **Breach Assessment Configuration** > **PI Data Elements**.
2. On the form, fill in the fields.

#### PI data element form

| Field | Description |
|---|---|
| Label | Category to which the data element belongs. For example, phone number, email address, and so on. |
| Name | Unique name to identify the data element. |
| Type | Type of preconfigured PI data element type with which the data element must be associated. |
| Application | Name of the application this data element applies to. This field is automatically set to **GRC: Privacy Case Management**. |
| Active | Option to activate the PI data element. |
| Applied to | Location of where the data element is applicable. The options are as follows:<br>◦ **All regions**<br>◦ **Specific to a region** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Description | Brief description of the data element. |

3. Select **Submit**.

### Create a region

Create geographic regions based on the data of the residents that is collected as a part of your business operations. Examples of regions are America, Europe, Asia Pacific, and so on.

#### Before you begin
Role required: sn_privacy_case.privacy_case_admin. This role must contain the user_admin role.

#### About this task
When you create a region, it is necessary to set the **Parent** field as empty.

#### Procedure
1. Navigate to **All** > **Privacy Case Management** > **Breach Assessment Configuration** > **Regions**.
2. Select **New**.
3. On the form, fill in the fields.
4. Select **Submit**.

### Create a jurisdiction for a region

Create jurisdictions for regions for data breach notification obligations as each obligation is broken down by jurisdiction. Jurisdiction can be created two levels below a region.

#### Before you begin
Role required: sn_privacy_case.privacy_case_admin. This role must contain the user_admin role.

#### Procedure
1. Navigate to **All** > **Privacy Case Management** > **Breach Assessment Configuration** > **Regions**.
2. Open the region for which you want to add jurisdictions.
3. Select the Locations related list.
4. Select **New**.
5. On the form, fill in the fields.
6. Select **Submit**.

## Using Privacy Case Management

You can use the Privacy Case Management application to report privacy cases and manage the lifecycle of a privacy case.

### Reporting a privacy case

Any user can report a privacy case or an event that needs the attention of the privacy team.

As a business user, you can report a case using one the following options:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Employee Center
- Privacy Workspace

### Report a privacy case from the Employee Center

Use the Employee Center to report any privacy breaches and complaints directly to the privacy teams. Reporting these cases helps to reduce and avert losses.

## Before you begin

Role required: sn_privacy.business_user

## Procedure

1. Navigate to **All** > **Self-Service** > **Employee Center**.
2. Select the **Risk & Compliance** tab.
3. Select **Report a privacy case**.
4. On the form, fill in the fields.
   See the Employee Center privacy case creation form for an explanation of each field.
5. To provide supporting material or evidence, select **Add attachments**.
6. Select **Submit**.

### Employee Center privacy case creation form

On the new privacy case form in the Employee Center, fill in the fields as appropriate.

**Report a privacy case form**

| Field | Description |
|---|---|
| Title | Name of the case. For example, `Customer records compromised by unprotected back-up database`. |
| Description | Brief description of the case. |
| Case type | Nature or type of the case. This field is automatically set to **Privacy case**. |
| Case subtype | Subtype of the case. For example, **Documentation Loss**. |
| Date of occurrence | Date the case occurred. For example, the case may have occurred on 18-02-2022. |
| Date of discovery | Date the case was discovered by you. For example, the case may have occurred on 18-02-2022, but was discovered only on 12-03-2022. |
| Personal information | |
| Categories of data subjects/individuals impacted | People impacted by the case. The choices are:<br>• **Customers**<br>• **Employees** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Report a privacy case form (continued)**

| Field | Description |
|---|---|
| Number of impacted individuals | Number of people impacted by the case. |
| Select the personal information attributes involved | Attributes of personal information that have been compromised in the case. |
| Provide additional personal information | Details of other personal information that is impacted by the breach. |
| Select the key stakeholders who own this application | Key stakeholders of the application. |
| Case origin | |
| Impacted business unit | Business unit that is impacted by the breach. |
| Impacted department | Department impacted by the breach. |
| Where the case occurred (location)? | Location of the case occurrence. For example, the location is **Japan**. |
| Where the case occurred (Sub-location)? | Sub location of the case occurrence. For example, the sub location is **Tokyo**. |

### Create a privacy case in the Privacy Workspace

Report any privacy breaches and complaints to help reduce and avert losses.

#### Before you begin

Role required: sn_privacy.analyst

#### About this task

At times, users can also report a case to the privacy teams using offline modes such as phone calls or emails. The privacy teams then create these cases in the Privacy Workspace and then attach the relevant details to the case.

#### Procedure

1. Navigate to **All** > **Privacy Workspace**.
2. Select the Privacy Case Management icon (  ).
3. Select **Create**.
4. Select **Case**.
5. On the form, fill in the fields.
   See the privacy new case form for an explanation of each field.
6. Select **Save**.

### Privacy new case form

On the new privacy case form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### New Privacy case form

| Field | Description |
|---|---|
| Number | Number of the case. This field is automatically set. |
| Title | Name of the case. For example, `Customer records compromised by unprotected back-up database`. |
| Type | Nature or type of case. This field is automatically set to **Privacy case**. |
| State | Workflow state of the case. This field is automatically set to **New**. |
| Requester | Person who reported the case. |
| Primary entity | Entity impacted by the case. Only the entities identified in the impacted areas are available for selection as the primary entity. |
| Sub-type | Sub type of case. For example, **Documentation Loss**. |
| Priority | Priority of the case. The choices are as follows:<br>• **1 - Critical**<br>• **2- High**<br>• **3 - Moderate**<br>• **4 - Low**<br>• **5 - Planning**<br>**Note:** The default value in this field is set to **Planning**. |
| Requested on behalf of | Name of the person on whose behalf you've created the case. |
| Entity owner | User who is the owner of the entity. This field is automatically set based on the entity selected in the Impacted areas related list. |
| Description | Brief description of the case. |
| Personal information | |
| Contains personal information | Field to decide if the breach contains personal information. The choices are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New Privacy case form (continued)**

| Field | Description |
|---|---|
| | • **To be decided**: Select this option if you're not sure if the breach has personal information.<br>• **Yes**: Select this option if the breach has personal information.<br>• **No**: Select this option if the breach doesn't have personal information. |
| Number of impacted individuals | Number of people impacted by the case. |
| Categories of data subjects/individuals impacted | Define who is impacted by the case. The choices are as follows:<br>• **Customers**<br>• **Employees** |
| Assignment | |
| Assignment group | Group assigned to the case.<br>**Note:** The assignment group is preconfigured to the case type during configuration setup. |
| Case analyst | Analyst who will analyze and work on the case. The case analyst is a part of the Assignment group. |
| Watch list | People who must be aware of the case. |
| Accountable executive | Executive who is accountable for the case. |
| Primary origin | |
| Location | Location where the case occurred. For example, the location is **Japan**. |
| Impacted business unit | Business unit that is impacted by the breach. |
| Source | Source of the case creation. This field is automatically set to **Manual** when the case is manually created. If the case is reported from the Employee Center, the field displays the source as **Employee Center**. |
| Additional source | Mode of how the case is reported when the case is created manually. This field is available only when **Manual** is selected from the **Source** field and the record is saved. The choices are as follows:<br>• **Email**<br>• **Phone** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New Privacy case form (continued)**

| Field | Description |
|---|---|
| Sub-location | Sub location of the case occurrence. For example, the sub location is **Tokyo**. |
| Impacted department | Department impacted by the case. The choices are as follows:<br>• **Finance**<br>• **HR**<br>• **IT**<br>• **Marketing**<br>• **Sales** |
| Source record | Source record of source object from where the case is created. For example, if the case is reported from risk events, then this field displays the name of the risk event from which the case is reported. |
| Schedule | |
| Date of occurrence | Date the case occurred. For example, the case may have occurred on 18-02-2022. |
| Date of discovery | Date the case is discovered by you. For example, the case may have occurred on 18-02-2022, but is discovered by the user only on 12-03-2022. |
| Reported date | Date the case is reported. |
| Case closure SLA | Expected date of case closure. |
| Investigation planned start | Planned start date to investigate the case. |
| Investigation actual start | Actual start date of case investigation. |
| Remediation planned start | Planned start date to remediate the case. |
| Remediation actual start | Actual start date of case remediation. |
| Investigation planned end | Planned end date to investigate the case. |
| Investigation actual end | Actual end date of case investigation. |
| Remediation planned end | Planned end date of case remediation. |
| Remediation actual end | Actual end date of case remediation. |
| Breach analysis | |
| Breach status | Status to indicate if a breach has occurred or not. The choices are as follows:<br>• **To be determined**: This is the default value.<br>• **Breach detected**: If the breach is confirmed. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New Privacy case form (continued)**

| Field | Description |
|---|---|
| | • **Future potential**: If the breach has not occurred but may occur in the future.<br>• **Not a breach**: When there is no breach detected. |
| Breach start | Date the breach started. This field only appears when **Breach detected** or **Future potential** is selected from the **Breach status** field. |
| Reporting status | Status of the case being reported to the regulators. This field is automatically set based on the reporting status of the regulations associated with the case. If a case has many regulations and even if one regulation is identified as reportable, then the reporting status of the case is set to **Reportable**. The default value of this field is **To be determined**. |
| Breach end | Date the breach ended. This field only appears when **Breach detected** or **Future potential** is selected from the **Breach status** field. |
| Breach significance identified | Date when the user identifies that the breach is significant. This field only appears when **Breach detected** or **Future potential** is selected from the **Breach status** field. |
| Root cause analysis | |
| Primary cause | Primary cause of the case occurrence. This field is automatically set to the primary cause that is selected in the Cause and consequences related list. |
| Related consequence | Consequences of the primary cause for the case. |
| Overall observations | Observations made regarding the case. |
| Remediation taken | Field to indicate if remediation measures have been taken to address the case. The choices are as follows:<br>• **Yes**<br>• **No** |
| Overall preventive measures | Preventive measures taken toward the case. |
| Activity | |
| Work notes (Private) | Notes or information regarding the case. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### New Privacy case form (continued)

| Field | Description |
|---|---|
| Additional comments (Customer visible) | Additional information regarding the case for the customers. |

## Case task workflow

Case tasks help you to collaborate with multiple teams to investigate, perform impact assessment to establish case criticality, and gather evidence to capture the details and responses for further review.

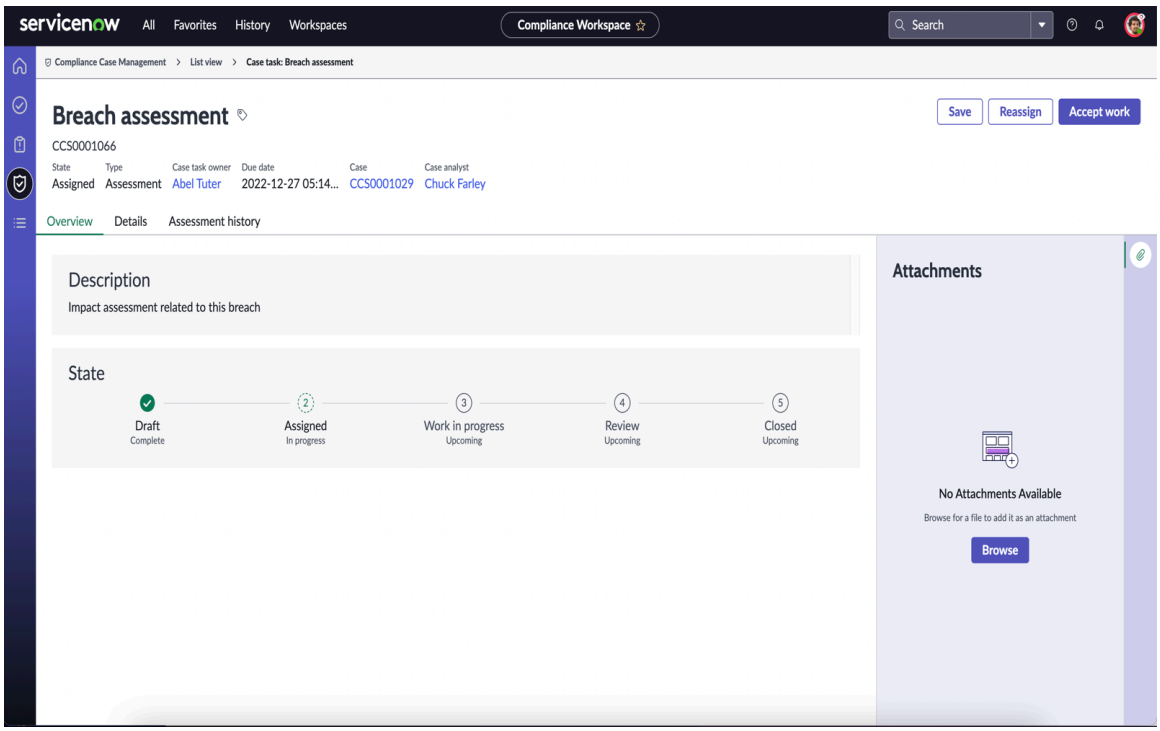
After a privacy case is reported, the privacy analyst can create case tasks and assign each of those tasks to various case task owners. The case task owners then work on the tasks and submit them for the case analyst to review. There are three types of case tasks:

- **Assessment**: This type of case task requires the case task owner to take an assessment and provide their responses. Case tasks that belong to this type can only be reassigned.
- **Investigation**: This type of case task requires the case task owner to provide their observations.
- **Others**: Like Investigation, this type of case task also requires the case task owner to provide their observations.

After case task owners work on a task, they submit the task for the case analyst to review.

The following image displays the life cycle of a case task.

### Case task workflow




## Create a case task

Create case tasks to work on the various tasks such as investigations, assessments, enquiries, gathering evidence, and so on required to analyse and work on the case that has been reported. Each case can have multiple case tasks that can be assigned to different owners from various teams.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_privacy_case.privacy_case_analyst

### About this task
After a case is reported to the privacy teams, a privacy case analyst can create case tasks and assign those tasks to the relevant owners to work on and provide the required inputs and responses.

### Procedure
1. Navigate to **All** > **Privacy Management** > **Privacy Workspace** > **Lists** > **Cases** > **All cases**.
2. Open the case for which you want to create a case task.
3. Select the Case task related list.
4. On the form, fill in the fields.
   See the privacy new case task form for an explanation of each field.
5. Select **Save**.
6. To assign the task to the case task owner, select **Assign task**.
7. Optional: In the confirmation dialog box, provide your notes.
8. Select **Move to assigned**.
   The state of the record changes to **Assigned** and is assigned to a case task owner.
9. Optional: To reassign the case task to another user before the case task is accepted by the case task owner specified by you, select **Reassign**.
   You can only reassign case tasks that are of type **Assessment**.
   a. In the Assignment group field, select the relevant group.
   b. In the **Case task owner** field, select a new owner.
   c. Select **Reassign**.

#### Case task form
On the new case task form, fill in the fields.

#### Case task form

| Field | Description |
|---|---|
| Number | Number of the case task. This field is automatically set. |
| Title | Name of the task being created for the case. For example, `Investigation for loss of data`. |
| Type | Type of task. The choices are as follows:<br>• **Assessment**: Use this option if you want to perform an assessment to collect responses from users regarding the case.<br>**Note:** Only case tasks with type Assessment type can be reassigned to a different task owner if required.<br>• **Investigation**: Use this option if you want to create a case task to perform any |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Case task form (continued)**

| Field | Description |
|---|---|
| | investigation for the case reported. For example, you may want to determine the type of data lost.<br>• **Others**: Use this option for any other type of task that you configure. |
| Assessment template | Assessment template to assess the case. This field appears only when **Assessment** is selected from the **Type** field.<br>**Note:** Each case type can be mapped to specific assessment templates during configuration. Only the templates mapped to the case are available for selection. For example, if the case type is **Financial**, then the assessment templates specific to the Financial type will be available for selection. You cannot select the same assessment template if there is already an open assessment with the assessment template that you have selected is being worked upon. |
| State | Workflow state of the case task. This field is automatically set to **Draft**. |
| Description | Brief description of the task. This description is useful for the user who works on the task. |
| Assignment | |
| Assignment group | Group that will work on the case task. Any user who belongs to the selected group can work on the case task if a case task owner is not specified. |
| Case task owner | Person who owns the case task. The user selected in this field must be a member from the assignment group. |
| Watch list | Users who must have the access to view the case task. |
| Schedule | |
| Due date | Date within which the case task must be completed. The due date must be before the date specified in the **Case closure SLA** field on the case form. |
| Accepted date | Date the case is accepted. |
| Created | Date the case is created and assigned to the case task owner. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Case task form (continued)**

| Field | Description |
|---|---|
| Task closure date | Date of the task closure. |
| Summary | |
| Observations | Observations you make about the case while working on the case task. |
| Activity | |
| Work notes (Private) | Worknotes for the case task. |
| Additional comments (Customer visible) | Comments related to the case task, if any. |

### Work on a case task

As a case task owner, accept the task, provide the details requested by the case analyst, and submit it for a review. If a case task is assigned to an assignment group, and not to a specific user, then any user who is a part of the assignment group can accept the task and work on it.

## Before you begin

Role required: sn_privacy_case.privacy_case_business_user

## About this task

If a case task is of type **Assessment**, a case requires the case task owner to take an assessment to determine losses incurred from a case. In this case, the task owner can accept the work and then take the assessment. If the case task is of type **Investigation** or **Others**, the case task owner can accept the task, provide their observations, and submit the case for review to the case analyst.

## Procedure

1. Navigate to **Self Service** > **Employee Center**.
2. Access your task from the **My tasks** module.
3. Open the task assigned to you.
4. Select **Accept work** .
5. In the confirmation dialog box, select **Accept work**.
6. Depending on your case task type, perform the following steps.

| Choice | Steps |
|---|---|
| If the task is of type Assessment | **a.** Select **Take assessment**.<br>**b.** Respond to the questions in the assessment.<br>**c.** Select **Submit**.<br>**d.** Save the **Save**. |
| If the task is of type Investigation or Others | **a.** In the Observations field, provide your comments.<br>**b.** Select **Save**.<br>**c.** Select **Ready for review**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Choice | Steps |
| --- | --- |
| | **d.** In the confirmation dialog box, provide your comments.<br>**e.** Select **Ready for review**. |

### What to do next

1. Create or manage an information object on a processing activity.
2. Add key stakeholders and send privacy assessments.
3. Add impacted areas to a case.
4. Add related areas to a case.
5. Add causes and consequences to a case.
6. Add regulations to a case.
7. Add issues to a case.

#### Reassign an assessment type case task

Reassign an **Assessment type** case task to another user. A case analyst or a case task owner can reassign a task to another case task owner, if required.

### Before you begin

Role required: sn_privacy_case.privacy_case_analyst, sn_privacy_case.privacy_case_business_user

### About this task

There are three types of case tasks and they are described as follows.

- **Assessment**: This type of case task requires the case task owner to take an assessment and provide their responses.
- **Investigation**: This type of case task requires the case task owner to provide their observations.
- **Others**: Like Investigation, this type of case task also requires the case task owner to provide their observations.

As a case analyst, after a task is assigned to a case task owner, you can reassign the task to another privacy business user. Possible reasons for reassignment can be that a case task is wrongly assigned or is not accepted by the case task owner and so on. You can reassign a task to privacy business users.

As a case task owner, you can also accept the task, start working on it, and then reassign the partially completed task to another user. When you reassign the partially completed case task to another user, the data that you have provided also gets copied over and is available when the new case task owner takes the assessment. This data can be modified by the new task owner.

**Note:** You can only reassign those case tasks that have the **Type** field set to **Assessment**.

### Procedure

1. Navigate to **Self Service** > **Employee Center**.
2. Access your task from the **My tasks** module.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Open the task that you want to work on.
4. Select **Reassign**.
   The Reassign case task dialog box appears.
5. In the **Assignment group** field, select the assignment group.
6. In the **Case task owner** field, select the owner.
7. Select **Reassign**.

### Review and close a case task

Review a case task after a case task owner provides their responses and observations for the case.

#### Before you begin

Role required: sn_privacy_case.privacy_case_analyst

#### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace**.
2. From the **Tasks** module, open the task to review.
3. Review the case task and then do one of the following.

| Choice | Steps |
|---|---|
| To request revision of the details provided by the case task owner | **a.** Select **Request revision**.<br>**b.** Provide your notes and comments.<br>**c.** Select **Request revision**. |
| To close the task as complete | **a.** Select **Complete**.<br>**b.** Provide your notes and comments.<br>**c.** Select **Close as complete**. |
| To close the task as incomplete | **a.** Select **Close as incomplete**.<br>**b.** Provide your notes and comments.<br>**c.** Select **Close as incomplete**. |
| To cancel the case task | **a.** Select **Cancel**.<br>**b.** Provide your notes and comments.<br>**c.** Select **Cancel**. |

### Add an impacted area to a privacy case

Add the impacted areas or objects that are affected by the privacy case or event in the Privacy Case Management application.

#### Before you begin

Role required: sn_privacy_case.privacy_case_analyst

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace**.
2. Select the list  icon.
3. Select **All Cases**.
4. Open the case for which you want to add an impacted area.
5. Select **New**.
6. On the **Impacted area** form, fill in the fields.

#### Impacted area form

| Field | Description |
|---|---|
| Case | Case for which you're adding the impacted areas. This field is automatically set to the case name. |
| Impacted area type | Type of the impacted area. For example, the location of the event or case. The choices are as follows:<br>◦ **Control**<br>◦ **Entity**<br>◦ **Location**<br>◦ **User**<br>◦ **Company**<br>◦ **Processing activity**<br>**Note:** You can also configure your own impacted area type. |
| Impacted area | Areas or objects that are affected by the case or event. This field is available only when a value is selected from **Impacted area type**. For example, **10065 East Harvard Avenue, Denver,CO**. |
| Title | Title of the impacted area. |
| Description | Brief description of the impacted areas or objects. |

7. Select **Save**.

#### Add a related area to a privacy case

Add the related areas that are related to a privacy case or event reported in the Privacy Case Management application.

### Before you begin

Role required: sn_privacy_case.privacy_case_analyst

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task
You can specify the related areas, such as policies, citations, control objectives, and risk events related to the privacy case or event reported. A privacy administrator can also configure the options for the related areas in the application setup.

### Procedure
1. Navigate to **All** > **Privacy Management** > **Privacy Workspace**.
2. Select the list  icon.
3. Select **All Cases**.
4. Open the case for which you want to add a related area.
5. Select **New**.
6. On the **Related area** form, fill in the fields.

**Related area form**

| Field | Description |
|---|---|
| Case | Case for which you're adding the related areas. This field is automatically set to the case name. |
| Related area type | Type of the impacted area. For example, any related risk event. The choices are as follows:<br>◦ **Citation**<br>◦ **Policy**<br>◦ **Control objective**<br>◦ **Risk event** |
| Related area | Areas that are related to the privacy case or event reported. This field is available only when a value is selected from **Related area type**. For example, **Employees education data loss**. |
| Title | Title of the related area. |
| Description | Brief description of the related areas. |

7. Select **Save**.

## Add causes and consequences to a privacy case

Define the root cause for the reported privacy case or event and its consequences on the organization using the Privacy Case Management application.

### Before you begin
Role required: sn_privacy_case.privacy_case_analyst

### About this task
You can add multiple causes to a privacy case and define a primary cause. Any privacy case can only have one primary cause. You can also add a cause that is suspected but not

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

confirmed. Apart from specifying the primary the cause, you can specify the consequence and any remediation measures taken to address the case.

### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace**.
2. Select the list  icon.
3. Select **All Cases**.
4. Open the case for which you want to add a cause and consequence.
5. Select **New**.
6. On the **Cause and consequence** form, fill in the fields.
   For a description of the field values on the **Cause and consequence** form, see Cause and consequence form.
7. Select **Save**.

### Cause and consequence form

Learn about the fields on the cause and consequence form. Use this form to define cause and consequence in the Privacy Case Management application.

On the view rule form, fill in the fields as appropriate.

**Cause and consequence form**

| Field | Description |
|---|---|
| Cause | Cause for the case or event. |
| Cause status | Status of the cause. The choices are as follows:<br>• **Suspected**: Select this option, if the cause isn't yet confirmed.<br>• **Confirmed**: Select this option, if the cause is confirmed. |
| Primary cause | Option to select the cause as primary. |
| Cause description | Brief description of the cause. |
| Consequences and actions | |
| Consequences | Consequences of the case or event. You can select multiple consequences for a reported case. |
| Actions taken | Any action or measures taken to address the case. |
| Summary | |
| Observations | Overall observations, if any. |

### Add a privacy regulation related to a case

Add the necessary regulations that are or can be impacted by the case that has been reported. In the ServiceNow platform, regulations are captured as authority documents.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Adding the regulations to the case enables you to identify which regulations are breached or violated and prevents penalties and fines.

### Before you begin
Role required: sn_privacy_case.privacy_case_analyst

### About this task
After you add the regulations, you can analyse the case to determine which regulations are violated. You can then mark the reporting status of the regulations as reportable, non-reportable, or potentially reportable. By default, all the regulations present in the system are displayed and the status of the regulations is set to **To be determined**.

### Procedure
1. Navigate to **All** > **Privacy Management** > **Privacy Workspace**.
2. Select the Tasks icon ( ).
3. Select **Cases**.
4. Open the case for which you want to add the regulations.
5. Select the Regulations related list.
   a. Select **Add**.
   b. Select the regulations to add.
   c. Select **Add**.
6. To set the reporting status of a regulation, select and open the regulation.
7. On the form, fill in the fields.

**Regulation form**

| Field | Description |
|---|---|
| Case | Case for which you're adding the regulation. This field is automatically set to the case name. |
| Reporting status | Status to determine if the regulation must be reported immediately, or in the future or does not require to be reported at all. The choices are as follows:<br>◦ **To be determined**: Select this option if the you're not sure if the violation must be reported.<br>◦ **Reportable**: Select this option if the violation must be reported.<br>◦ **Non-reportable**: Select this option if the violation does not need to be reported.<br>◦ **Potentially reportable**: Select this option if you think that the violation can be reported in the future based on the case investigation. |
| Authority document | Authority document which forms the regulation. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Lodgement date | Date the regulation is reported to the regulators. |
| Description | Brief description of the regulation violation based on your analysis. |

8. Select **Save**.

### Add or create an issue for a privacy case

Identify and manage issues related to the impacted areas for the reported privacy case. You can also create issues from the Privacy Case Management landing page.

#### Before you begin

Role required: sn_privacy_case.privacy_case_analyst

#### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace**.
2. Select the list  icon.
3. Select **All Cases**.
4. Open the case for which you want to add an issue.
5. Select the Issues related list and do one of the following.

| Option | Action |
|---|---|
| To add an existing issue | **a.** Select **Add**<br>**b.** Select the issues you want to add.<br>**c.** Select **Add**. |
| To create an issue | Refer to the new issue creation form. |

6. Select **Save**.

### Export a privacy case as a PDF

Export a privacy case as a PDF to easily share it with various stakeholders.

#### Before you begin

Role required: sn_privacy_case.privacy_case_analyst

#### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace**.
2. Select the list  icon.
3. Select **All Cases**.
4. Open the case that you want to export as a PDF.
5. Select the More actions icon on the top right corner.
6. Select **Export PDF**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. Select the appropriate PDF template.
8. Select **Export**.

### Send an email from a privacy case

Send emails from a privacy case to seamlessly communicate with various stakeholders and regulators and gather more information about the case. All the emails sent and received are stored in the Privacy Case Management application.

#### Before you begin

Role required: sn_privacy_case.privacy_case_analyst

#### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace**.
2. Select the list  icon.
3. Select **All Cases**.
4. Open the case that from which you want to send an email.
5. Select the More actions icon on the top right corner.
6. Select **Compose Email**.
7. Draft the email.
8. Select **Send Email**.

### Initiate a breach assessment from a case

Initiate a breach assessment from a privacy case to capture the details of breach, the type of data that is impacted, and so on. These details help the privacy analyst to identify if the breach must be notified to a regulator.

#### Before you begin

Role required: sn_privacy_case.privacy_case_analyst

#### Procedure

1. Navigate to **All** > **Privacy Management** > **Privacy Workspace**.
2. Select the list  icon.
3. Select **All Cases**.
4. Open the case that from which you want to initiate the breach assessment.
5. Select **Initiate breach assessment**.

## Privacy Case Management integration for RadarFirst

RadarFirst specializes in privacy and incident response solutions, particularly in the context of data breach incidents. RadarFirst helps organizations manage and respond to data breaches and privacy incidents effectively.

RadarFirst provides tools for incident response planning, risk assessment, and compliance with data breach notification laws.

In the event of a privacy breach, if you have integrated with RadarFirst by activating the sn_privacy_rf plugin and have an account can submit the breach details. RadarFirst then

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

analyzes the breach in accordance with all relevant privacy regulations for all the locations involved, determining whether it is necessary to notify a regulator about the breach. This notification helps the privacy teams to get their actionable items and act as necessary.

To configure the Privacy Case Management integration for RadarFirst, follow the Guided set up steps and navigate to **Privacy Case Management** > **RadarFirst Integration** > **RadarFirst Integration Guided Setup**.

## Privacy Case Management reference information

Reference topics provide additional information about the Privacy Case Management application including tables.

### Components installed with Privacy Case Management

Several types of components are installed with installation of the Privacy Case Management application, including tables, user roles.

## Roles installed

Privacy Case Management roles.

| Role | Description | Contains roles |
|---|---|---|
| Privacy case business user [sn_privacy_case.privacy_case_business_user] | To create a Privacy case from Employee center. | sn_grc_case_mgmt.grc_case_business_user |
| Privacy case analyst [sn_privacy_case.privacy_case_analyst] | Work on the privacy case assigned to them. As part of investigating privacy cases, they can review the breach assessment and associate the Information objects, key stakeholders Impacted areas, related areas, Causes and Consequences, Regulations and Issues which are assigned to them. | sn_privacy_case.privacy_case_analyst, sn_grc_case_mgmt.grc_case_manager |
| Privacy case manager [sn_privacy_case.privacy_case_manager] | Privacy cases can be classified into multiple groups and for every group there can be a manager. A privacy case manager can assign or reassign privacy cases to privacy analysts who are part of the same group. Privacy case manager has the same access as that of the privacy analyst. | sn_privacy_case.privacy_case_analyst, sn_grc_case_mgmt.grc_case_manager |
| Privacy case admin [sn_privacy_case.privacy_case_admin] | Configure the privacy case type that has configurations such as privacy workflow configurations, assignment rules, sub types, assessment templates. They can also | sn_grc_case_mgmt.grc_case_admin, sn_privacy_case.privacy_case_manager |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role | Description | Contains roles |
|---|---|---|
| | configure breach assessment configurations. | |

## Tables installed

### Privacy Case Management application tables

| Table | Description | Application |
|---|---|---|
| GRC case (sn_grc_case_mgmt_case) | Stores all the case details. | GRC: Core Case Management |
| Case classification (sn_grc_case_mgmt_case_classification) | Stores the case classifications. | GRC: Core Case Management |
| Case task (sn_grc_case_mgmt_case_task) | Stores all the case tasks created on for the Privacy cases. | GRC: Core Case Management |
| Case type (sn_grc_case_mgmt_case_type) | Stores the case type and case subtype details. | GRC: Core Case Management |
| Cause sn_grc_case_mgmt_cause | Stores the causes added to the library and mapped at the case level. | GRC: Core Case Management |
| Cause and consequence sn_grc_case_mgmt_cause_consequence | Stores the causes and consequences mapped at the case level. | GRC: Core Case Management |
| Consequence sn_grc_case_mgmt_consequence | Stores the Consequences added to the library and mapped at the Case level. | GRC: Core Case Management |
| GRC core case sn_grc_case_mgmt_core_case | Stores the details of core functionality of the Case. | GRC: Core Case Management |
| Impacted area sn_grc_case_mgmt_impacted_area | Stores the impacted areas mapped at the Case level. | GRC: Core Case Management |
| Case Task to Assessment Instance sn_grc_case_mgmt_m2m_case_task_assessment_instance | Stores Assessment details on Case tasks of type assessment. | GRC: Core Case Management |
| Issue to Case sn_grc_case_mgmt_m2m_issue_to_case | Stores the issues mapped to the Case record. | GRC: Core Case Management |
| Regulation sn_grc_case_mgmt_regulation | Stores the regulations mapped at the Case level. | GRC: Core Case Management |
| Related area sn_grc_case_mgmt_related_area | Stores the related areas associated with the Case. | GRC: Core Case Management |
| Privacy case sn_privacy_case_privacy_case | Stores Privacy case records. | Privacy Case Management |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Privacy Case Management application tables (continued)**

| Table | Description | Application |
|---|---|---|
| Information object to privacy case sn_privacy_case_m2m_information_object_to_case | Stores the Information object records mapped at Case level. | Privacy Case Management |
| Key stakeholders to case sn_privacy_case_m2m_key_stakeholders_to_case | Stores the Key stakeholders records mapped at Case level. | Privacy Case Management |

## Privacy Management reference

Reference topics provide additional information such as tables, and roles that are installed with the Privacy Management application. These topics also provide supporting information.

### Tables installed with Privacy Management

Tables are added with activation of GRC: Privacy Management.

**Tables installed**

| Table | Description |
|---|---|
| Assessment configuration [sn_privacy_assessment_configuration] | Privacy manager or admin can configure the rules for auto creating the processing activity on an assessment response. This table stores the assessment configuration rules on assessment template. |
| Control Objective to Processing Activity [sn_privacy_m2m_policy_statement_processing_activity] | Each processing activity can be associated to the applicable control objectives. This table enables tracking the processing activity to CO relationships. |
| Control to Processing Activity [sn_privacy_m2m_control_processing_activity] | Stores many-to-many relationships between controls and processing activity. |
| Entity Type to Assessment Instance [sn_privacy_m2m_profile_type_assessment_instance] | Privacy users can send multiple privacy assessments on Entity Type. This table enables the privacy assessments to processing activity relationships. |
| Information object to processing activity [sn_privacy_m2m_information_object_processing_activity] | Each processing activity can be associated to applicable Information objects. This table enables tracking the processing activity to IO relationships. |
| Privacy Unique User Usage [sn_privacy_unique_user_usage] | Collects the unique count of users who are using GRC Privacy Management tables. |
| Processing activity | Extends task table [sn_grc_item] and stores processing activities. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tables installed (continued)**

| Table | Description |
|---|---|
| [sn_privacy_processing_activity] | |
| Processing activity hierarchy<br><br>[sn_privacy_m2m_pa_pa] | Personal data can be moved from one processing activity to another processing activity. This table stores the upstream and downstream processing activities information for each processing activity. |

## Roles installed with Privacy Management

The GRC: Privacy Management application installs the roles for the privacy analyst, the privacy manager, and the privacy administrator to perform their respective tasks.

**Roles and their descriptions**

| Role title [name] | Description | Contains roles |
|---|---|---|
| Privacy Analyst<br><br>(sn_privacy.analyst) | Privacy analysts are responsible for managing the privacy compliance posture of the processing activities owned by them. They perform the following tasks:<br>• Assess the processing activities regularly by sending and reviewing privacy impact assessments.<br>• Work with the management and business users to identify and manage controls related to a processing activity.<br>• Manage and resolve the concerns of business users about compliance-related issues and policy exceptions.<br>• Test and monitor control effectiveness. | • sn_grc_workspace.task_reader<br>• sn_risk_advanced.ara_approver<br>• sn_risk_advanced.ara_assessor<br>• sn_risk.user<br>• sn_compliance.user<br>• sn_privacy_case.privacy_case_analyst |
| Privacy Manager<br><br>(sn_privacy.manager) | Privacy managers are responsible for managing the overall organization level privacy compliance posture. They perform the following tasks: | • sn_compliance.manager<br>• sn_privacy.analyst<br>• sn_risk.manager<br>• sn_grc_workspace.task_admin<br>• sn_compliance.attestation_creator |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles and their descriptions (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| | • Develop and implement privacy regulations, authority documents, and policies.<br>• Review privacy regulatory requirements and policies.<br>• Design and monitor controls to deal with violations of privacy regulations and internal policies.<br>• Plan privacy programs and scope entities.<br>• Creating privacy impact assessment templates.<br>• Continuously monitor control effectiveness and recommend effective improvements.<br>• Supervise the privacy compliance team.<br>• Report to management and the Board of Directors on compliance posture.<br>• Discover who is implementing privacy regulation for the first time in their organization. | • sn_grc_reg_change.manager<br>• sn_privacy_case.privacy_case_manager |
| Privacy Admin<br><br>(sn_privacy.admin) | Privacy administrators administer the privacy policy and compliance management. Users assigned this role are responsible for configuring privacy management solutions as per the privacy team's requirements. They perform the following tasks:<br>• Configure privacy impact assessments and automated flows to trigger assessments<br>• Configure rules to auto-create processing activities out of privacy screening assessments. | • sn_privacy.manager<br>• sn_risk_advanced.ara_admin<br>• sn_compliance.admin<br>• sn_privacy_case.privacy_case_admin |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles and their descriptions (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| | • Monitor the Now Platform dependencies with other applications and modules.<br>• Can read the scripts under Processing activity script configurations related list. | |
| Privacy assessment responder sn_privacy.assessment_responder | Privacy assessment responders can respond to the privacy assessments as key stakeholders. They can also raise privacy requests from the portal. | • sn_grc_workspace.task_reader<br>• canvas_user |
| Privacy business user sn_privacy.business_user | Privacy business users can edit the assigned processing activities in the Discover state, and also respond to the assessments. | • sn_grc_workspace.task_reader<br>• canvas_user<br>• sn_privacy_case.privacy_case_business_use<br>• sn_grc.business_user |
| Privacy Developer sn_privacy.developer | Privacy developers can write custom scripts | sn_privacy.admin |

## Privacy Management email notifications

Reminders enable relevant users to perform their assessments and complete the tasks associated with them.

By default, the Privacy Management application includes the following types of email notifications.

- Email notifications to the entity owner for privacy screening assessment.
- Email notifications to the entity owner for privacy impact assessment.
- Email notification received for Entity owner for when Privacy Assessment is cancelled when Assessment is in Open state.
- Email notification received for Entity owner for when Privacy Assessment is cancelled when Assessment is in Work-in-progress state.

The following table describes the recipient list of notifications and the associated conditions when a notification is sent.

**Notifications sent in the Privacy Management application**

| Notification | Condition | Recipients |
|---|---|---|
| Privacy assessment notification: New assessment on Privacy Screening Assessment | When a new privacy screening assessment is initiated. | Entity owner |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Notifications sent in the Privacy Management application (continued)**

| Notification | Condition | Recipients |
|---|---|---|
| Email notification sent to the entity owner for Privacy Impact Assessment. | When an entity owner receives a Privacy Impact Assessment. | Privacy manager |
| Email notification sent to the entity owner when Privacy Assessment is canceled when the assessment is in **Open state**. | When a privacy assessment is canceled and the assessment is in **Ready to take** state. | Entity owner |
| Email notification sent to the entity owner when Privacy Assessment is canceled when Assessment is in **Work In progress** state. | When a privacy assessment is canceled and the assessment is in **Work in progress** state. | Entity owner |
| Remainder email notification sent to the entity owner when the Privacy Assessment is in the due date. | Reminder email for when the assessment is due. | Entity owner |
| Overdue email notification sent to the entity owner when Privacy Assessment is overdue. | Overdue email | Entity owner |

## Uses of a processing activity in Privacy Management

A processing activity is a record that processes personal data. Examples of such records are a business process or a business application of an organization. Processing activities enable the privacy management teams to understand how personal information is being processed or used.

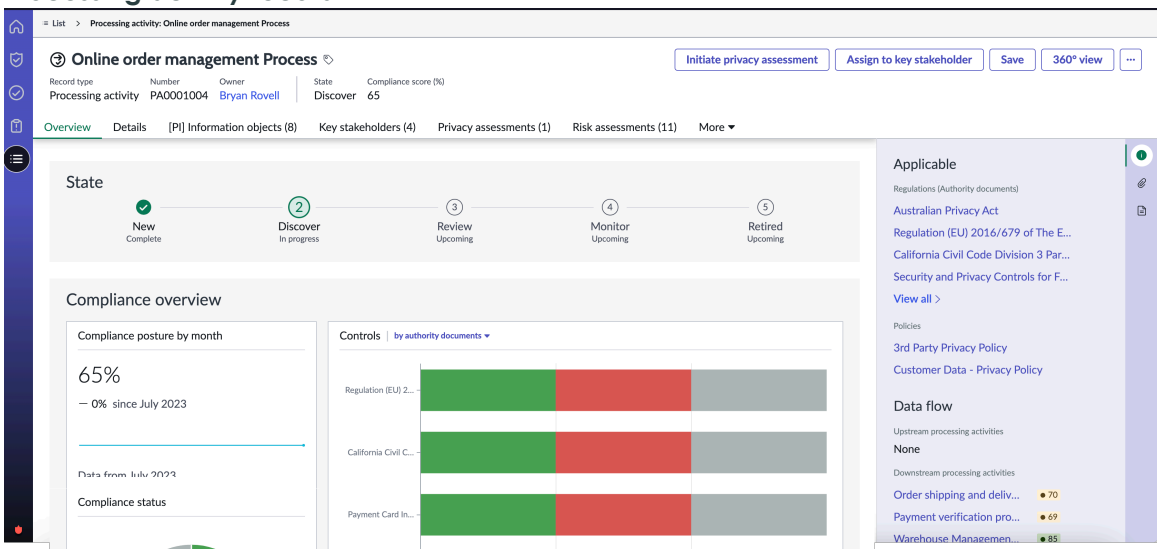
To understand more details about a processing activity, refer to Processing activities. A processing activity helps the privacy teams to record the following details:

- Processing activity details such as the business unit it belongs to, data subject type, data storage location, and so on.
- [PI] Information objects that are being processed as a part of this processing activity.
- Past and ongoing privacy assessments.
- Controls that are applied to the processing activity and the respective control attestation responses.
- Issues and policy exceptions associated with this processing activity.

The following image shows the Overview tab of a processing activity.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Processing activity record




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Workflow of a processing activity

A processing activity workflow helps the privacy analysts to manage the life cycle of a processing activity.

The following section explains the different stages of the processing activity workflow.

**Note:** Privacy analysts who do not own the processing activity can only view the processing activity. They cannot edit it.

## New

This is a state to confirm if the business application, business process, vendors, or business service must be considered for determining privacy compliance. A processing activity is in this state only when it is created manually. A privacy manager or a privacy analyst can create a processing activity manually and then confirm it as a processing activity based on their analysis. In this stage, the following fields of the processing activity can be modified:

- **Name**
- **Justification**
- **Privacy analyst**
- **Entity**: Only when this field is filled, and the processing activity form is saved. After saving the form, the privacy manager or a privacy analyst can move the processing activity the **Discover** state.

## Discover

In this state, the privacy manager or the privacy analyst, who owns the processing activity, can understand further details about the processing activity such as, why and how a processing activity is processing personal information. These details are collected by sending privacy assessments. Based on the responses, they apply the right set of controls. The following is the list of activities that can be performed on the processing activity form in this state.

- Send privacy assessments.
- Update the processing activity **Details** section based on the assessment responses.
- Assign the processing activity to one of the key stakeholders for the key stakeholders to update the details, the PI-tagged information objects, and the key stakeholders.

  **Note:** You can assign the processing activity to those users who have the sn_privacy.business_user role.

- Review the controls applied based on the privacy assessment responses.
- Add or remove additional controls as necessary.

The processing activity then moves to the **Review** state.

## Review

In this state, the privacy manager or the privacy analyst, who owns the processing activity, sends control attestations and reviews the compliance posture based on the attestation responses and issues that are created due to non-compliant controls. The following is the list of activities performed on the processing activity form by a privacy manager or the privacy analyst who owns the processing activity.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Update the processing activity Details section based on the assessment responses.
- Associate information objects and capture additional details related to the information objects based on the assessment responses.
- Review the controls applied automatically based on the privacy assessment responses, and add or remove additional controls as necessary.
- Send control attestations and track issues and policy exceptions.

### Monitor

This is a state to track the processing activity for continuous monitoring. The indicator functionality is used for continuous monitoring. When the processing activity is in this state, the privacy analyst can move the processing activity back to **Discover** or **Review** state based on the processing activity updates that must be assessed by the privacy analyst or the privacy manager. The following is the list of activities that can be performed on the processing activity form by a privacy manager or the privacy analyst who owns the processing activity.

- Auto execution of indicator functionality to continuously monitor controls associated with processing activity.
- Create, manage issues, and track issues.

**Note:** When a new privacy assessment is sent for a processing activity while it is in the **Monitor** state, the system automatically moves the processing activity to the **Discover** state.

### Retire

This is a state to retire the processing activity when the respective business application or business process is no longer used in the organization. When moved to this state, all the controls associated with the processing activity are retired. The privacy team cannot make any updates to a processing activity in the retired state. When an entity gets inactivated, the related processing activity is also automatically moved to the Retired state.

## Domain separation in Privacy Management

This is an overview of domain separation and the Governance, Risk, and Compliance application Privacy Management. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

### Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

For more information on support levels, see Application support for domain separation.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Overview

Domain separation is best for those customers who:

- Need to enforce absolute data segregation between business entities (data separation).
- Customize business process definitions and user interfaces for each domain (delegated administration).
- Maintain some global processes and global reporting in a single instance.

These users can choose to expand or collapse the domain scope to show or hide data from other domains.

**Note:** Users always have access to data from domains that have been explicitly granted to them by domain visibility.

## How domain separation works in GRC

- While GRC supports separation of data, separation of logic and process is not fully supported.

- Many types of records in GRC are automatically generated through user processes. Entities, controls, risks, indicators, control tests, and processing activities are all fields that can be generated automatically. For records that are automatically generated (and for any GRC record that is manually generated), the domain of the record is the same as the domain of the user responsible for creating or generating the records.

  Automatic generation should be kept in mind when working in a domain-separated GRC implementation. Users should be sure that they are creating or generating records at the right domain level so that they are visible to the right set of users.

  For example, suppose you have a domain hierarchy that has Global at the top level followed by Top domain. Top domain, in turn, has two sub domains: Domain A and domain B.

- If you have an entity that you want to send a privacy assessment that must assessed by users in domains A and B, the entity should be generated or manually created at the global level. If the entity is created in Domain B, you will not be able to recreate the entity in Domain A due to indexing.
- If you have an entity that you want to be assessed by users in Top and Domain A, you can create the entity in Domain A.

Unless the entities are in the Global domain, users should not assign entities in a higher domain to users in a lower domain. In the example above, if you have an entity in the TOP domain, you should not assign it for privacy assessment to users in Domains A or B since those users would not have access to the assessment; thus the assessment questionnaire would not be generated.

Similarly, users should not assign control objectives and risk statements in a higher domain to attestations and assessments in a lower domain. Otherwise the attestation or assessment questionnaire would not be generated.

## Use case

GRC data for IT can be separated from the GRC data of other departments. Each business area using the GRC application can have separate data that cannot be shared with other

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

departments. Therefore each department can have its own entities, policies, controls, risks, and so on.

When looking at a control from the IT domain, the user can choose to expand the domain scope to show values from the Finance domain or collapse the domain scope to show only controls that match the IT domain.

By default, domain separation adds a domain field to the Task `[task]` and Configuration Items `[cmdb_ci]` tables and their extensions.

You can extend domain separation to any new tables you create by adding a `sys_domain` field to the table's dictionary definition. By default, the system only domain-separates platform and baseline application tables where appropriate.

**Warning:** ServiceNow does not recommend domain separating platform tables (any table with the sys_ prefix such as the Dictionary Entry `[sys_dictionary]` and Dictionary Entry Override `[sys_dictionary_override]` tables) because it can produce unexpected results.

In this use case, client scripts, business rules, workflows, processes, and so on can be domain-separated.

While the behavior offered with domain separation provides multi-tenancy support, multi-tenancy is still contained within a single instance. This means that some global properties, some global data, and some global processes are shared across all domains. For example, the system's "Remember me" option on the login page is global and cannot be specified per domain.

If you need complete and total separation of all system properties and do not require global reporting or global processes, separate instances are the best option.

## Reporting for Privacy Management

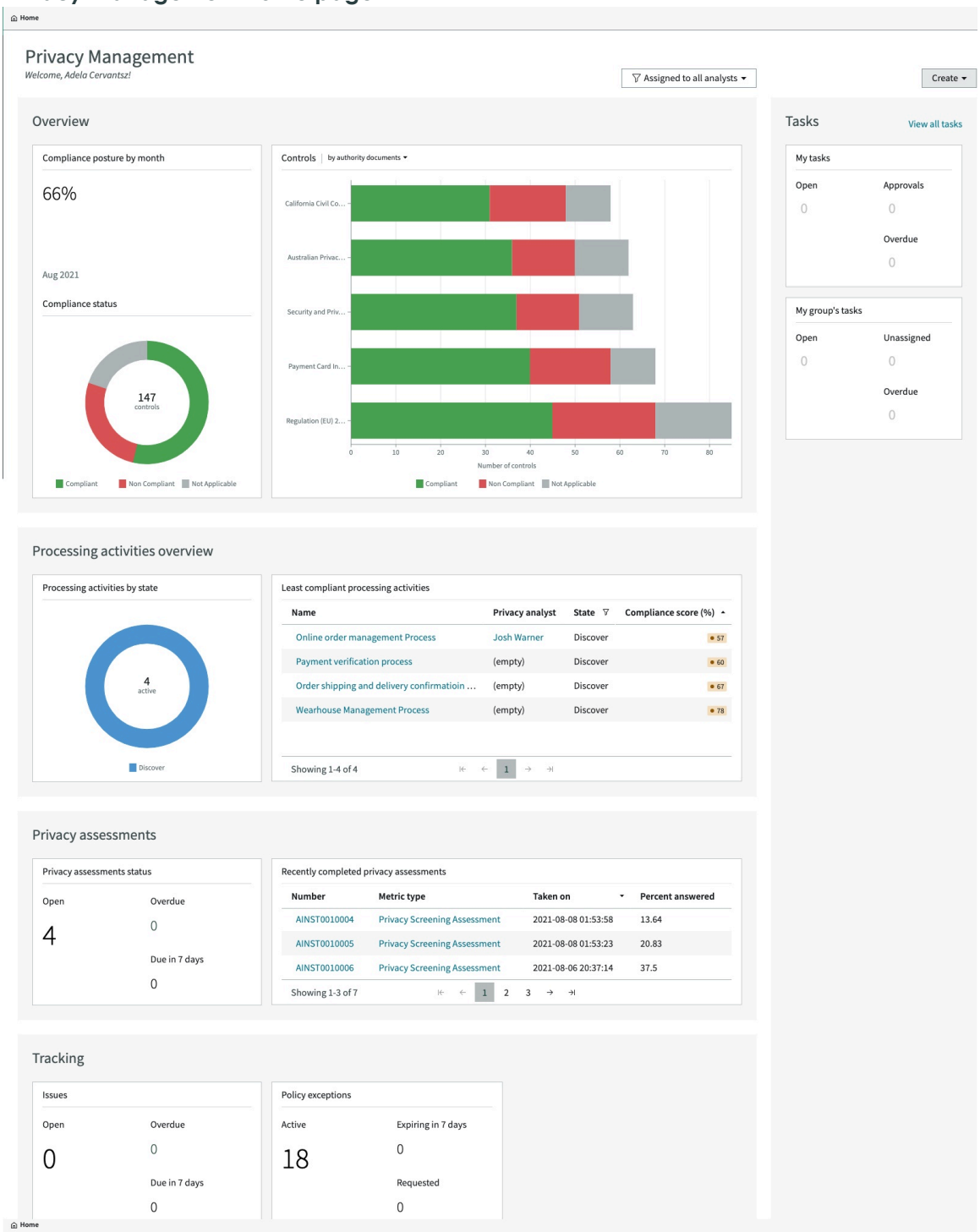
The Privacy Management reports are available as overview pages in the various records.

### Privacy Management home page

The Privacy Management home page provides an overview of the complete privacy risk and compliance posture with details such the overall compliance score and trend, privacy risk assessment status, privacy impact assessment status, control attestations, issues-specific status, and privacy-specific regulatory change tasks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Privacy management home page




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Required roles

To view the home page, you must have sn_privacy.manager and the sn_privacy.analyst roles.

## Use cases

For examples of how different people in your organization would use this home page, see the following use cases.

| User | Dashboard use |
|---|---|
| Privacy manager | The privacy manager can view and understand the privacy compliance posture considering all the processing activities and privacy assessments. They can also view the privacy team's tasks. |
| Privacy analyst | The privacy analyst can view and understand the privacy compliance posture considering only the processing activities assigned to the privacy analyst. They can also access the tasks that need their attention. |

## Indicators

The processing activity compliance score percentage indicator shows the compliance score percentage of the processing activity.

## Breakdowns

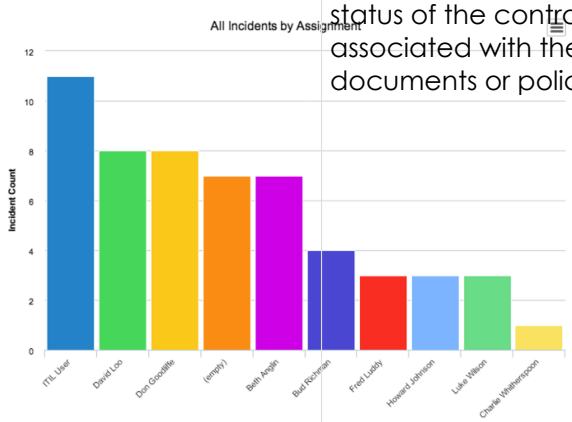
- Processing activity
- Privacy analyst

## Reports

This dashboard displays the following reports:

| Title | Type | Description |
|---|---|---|
| Compliance posture by month | Trend chart  | Compliance posture by month is plotted by referring to the overall compliance score across all the processing activities. |
| Compliance status | Donut  | Provides the compliance status of all the controls across all the processing activities. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Title | Type | Description |
|---|---|---|
| Controls (by authority documents or by policies) | Bar chart   | Provides the compliance status of the controls that are associated with the authority documents or policies. |
| Processing activities by state | Donut  | Shows the active processing activities breakup by the following states:<br>• New<br>• Discover<br>• Review<br>• Monitor |
| Least compliant processing activities | List report  | Shows the list of least compliant processing activities. |
| Privacy assessments status | Single score   | Shows the number of assessments that are open, overdue, and approaching due date. |
| Recently completed privacy assessments | List report  | Shows the list of recently completed privacy assessments. |
| Issues | Single score   | Shows the number of issues that are open, overdue, and approaching due date. |
| Issues by priority | Donut  | Shows the issues by their priority. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

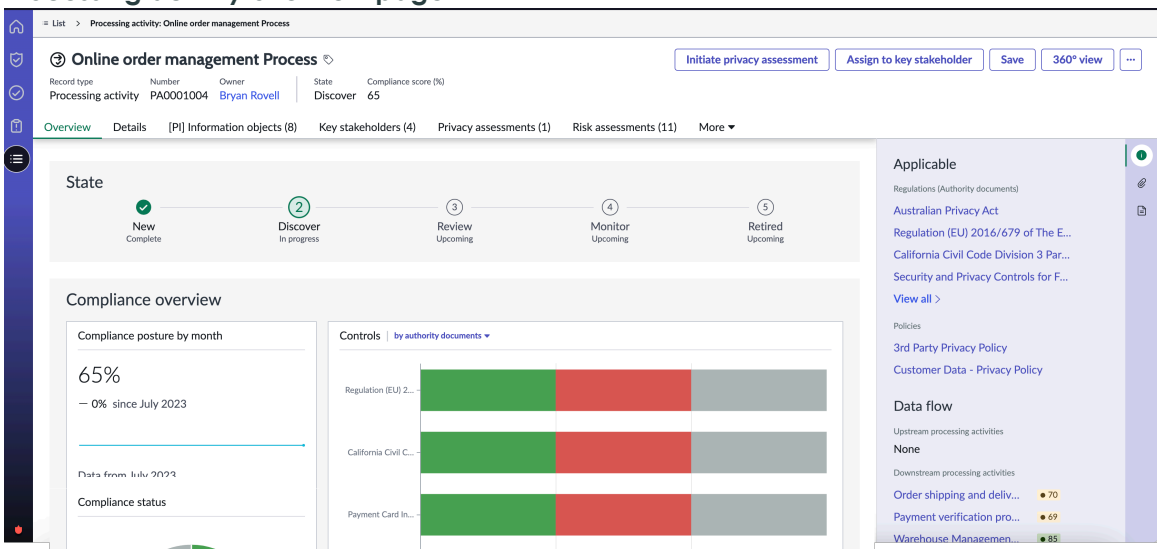
| Title | Type | Description |
| --- | --- | --- |
| Policy exceptions |  Single score | Shows the number of policy exceptions that are active, expiring, and requested. |
| By risk rating |  Donut | Shows the policy exceptions by their risk ratings. |
| Indicators |  Single score | Shows the number of open and failed indicators. |
| Attestations |  Single score | Shows the number of attestations that are open, overdue, and approaching due date. |

## Processing activity overview page

The processing activity overview page provides the privacy risk and compliance posture for a processing activity. This page contains details such the overall compliance score, and trends, privacy criticality assessment scores and risk heatmap based on privacy risk assessments, privacy assessment status, control attestations and issues-specific status.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Processing activity overview page




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Required roles

To view the home page, you must have sn_privacy.manager and the sn_privacy.analyst roles.

## Use cases

For examples of how different people in your organization would use this home page, see the following use cases.

| User | Dashboard use |
|---|---|
| Privacy manager and Privacy analyst | The privacy manager and the privacy analyst can view and understand the privacy compliance posture of the given processing activity. |

## Indicators

**Processing activity compliance score percentage**: Compliance score percentage of processing activity.

## Breakdowns

- Processing activity
- Privacy analyst

## Risk overview

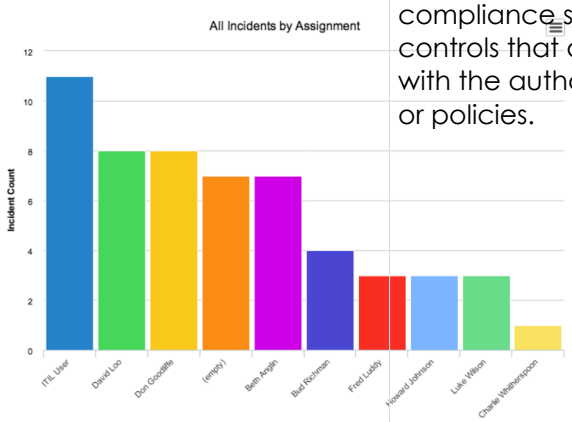
The risk overview section displays the processing activity criticality score, the number of high risks with no controls, the details of the on-going risk assessments, and the risk heatmap.

## Reports

This dashboard displays the following reports:

| Title | Type | Description |
|---|---|---|
| Compliance posture by month |  Trend chart | Compliance posture by month is plotted by referring to the processing activity compliance score. |
| Compliance status |  Donut | This report provides the compliance status of all the controls for the processing activity. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Title | Type | Description |
|---|---|---|
| Controls (by authority documents or by policies) | Bar chart   | This report provides the compliance status of the controls that are associated with the authority documents or policies. |
| Privacy assessments status | Single score   | Shows the number of assessments that are open, overdue, and approaching due date. |
| Recently completed privacy assessments | List report  | Shows the list of recently completed privacy assessments. |
| Issues | Single score   | Shows the number of issues that are open, overdue, and approaching due date. |
| Issues by priority | Donut  | Shows the issues by their priority. |
| Policy exceptions | Single score   | Shows the number of policy exceptions that are active, expiring, and requested. |
| By risk rating | Donut  | Shows the policy exceptions by their risk ratings. |

## Regulatory Change Management

The ServiceNow® Regulatory Change Management application enables you to check upcoming regulatory changes, assess their impact, and implement risk and compliance-related changes. The application ensures overall regulatory compliance.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

| | | |
|---|---|---|
| **Explore**<br>• Exploring Regulatory Change Management application<br>• Regulatory Change Management workflow | **Set up**<br>Download and install Regulatory Change Management | **Configure**<br>• Regulatory alerts<br>• Impact assessments for the regulatory event alerts<br>• Manage the regulatory change tasks<br>• Manage the source document import tasks<br>• Create an action task<br>• Create an issue related to the regulatory tasks<br>• Set up the RSS feeds<br>• Administration module<br>• Map the taxonomy |
| **Develop**<br>•<br>• Developer documentation | **Troubleshoot**<br>• Ask or answer questions in<br>• Search the Known Error Portal<br>• Contact Customer Service | |

## Exploring Regulatory Change Management application

The Regulatory Change Management application provides a framework and guidelines to integrate with third-party regulatory intelligence providers. It provides a centralized process for managing regulatory changes and ensures compliance with external regulations.

### Regulatory Change Management application

Various regulatory actions, rulings, and guidance documents are issued in the regulatory world. It is important to track regulatory change information and know how it impacts your organization.

The Regulatory Change Management application enables you to manage your upcoming regulatory changes efficiently. The application provides structured workflows that assess the applicability of the regulatory changes, that assess their impact, and that implement risk and compliance-related changes.

The Regulatory Change Management application works with the following types of components:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Integration component: The regulatory intelligence partners typically provide the integration component. Through this integration, you can consume regulatory alerts into your ServiceNow® instance.
- Application framework component: The Regulatory Change Management application has an application framework component. This component provides structured workflows so that you can analyze and process regulatory alerts that are received in the regulatory alerts table.

The Regulatory Change Management application consists of the following key functions:

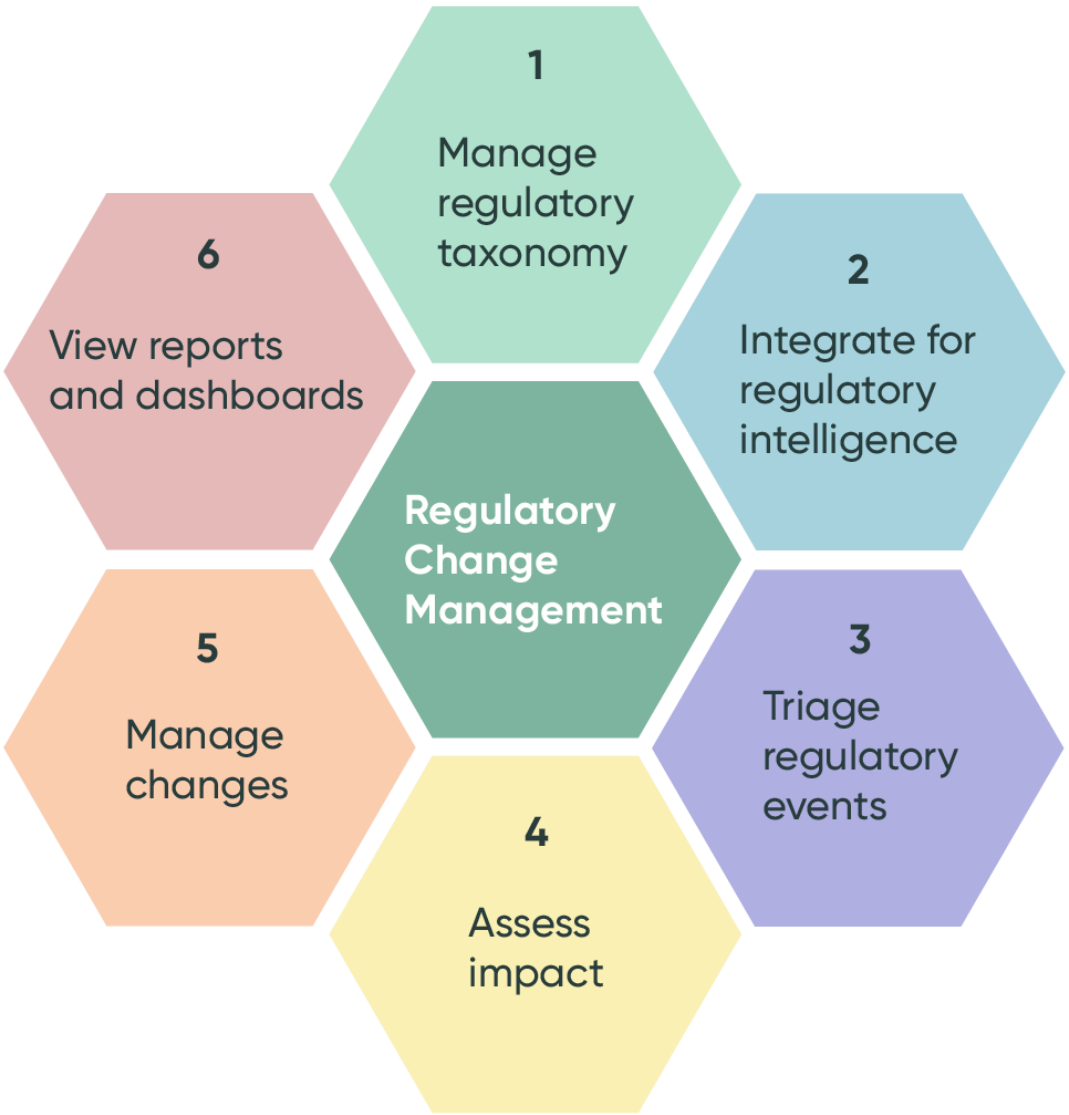
1. Manage regulatory taxonomy: Create an internal regulatory taxonomy that is specific to the ServiceNow platform. Map the taxonomy with the external taxonomies that are provided by third-party regulatory intelligence providers for standardization. The internal taxonomy contains the following design elements:
   - Content Type
   - Jurisdiction
   - Regulatory Body
   - Sector
   - Theme

   These elements are created and mapped with the external taxonomy during the setup process.
2. Integrate for regulatory intelligence: Integrate with third-party regulatory intelligence providers and consume the alerts into your ServiceNow instance at regular intervals. Monitor regulatory data in a rapid and complex changing environment.
3. Triage regulatory events: Analyze the regulatory alerts and identify the regulatory events that are relevant to your organization.
4. Assess impact: Assess the impact of regulatory events by using configurable impact assessment methodologies.
5. Manage changes: Identify changes that should be done. These changes are implemented through the following action tasks:
   - Update underlying GRC objects, such as policies, processes, risks, and controls in the regulatory library.
   - Update existing citations or import new citations from the providers in the regulatory library.
6. View reports and dashboards: Assess the state of the regulatory compliance by using reports and dashboards. Maintain an audit trail of the compliance activities.

These component functions are illustrated in the following image:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Key functions of the Regulatory Change Management application**




## User roles in Regulatory Change Management

Stakeholders in the Regulatory Change Management application have different roles and responsibilities.

The Regulatory Change Management application roles are installed with the activation of the GRC: Regulatory Change Management application. The application involves the following types of roles.

| Role titles and names | Description | Available roles |
|---|---|---|
| RCM Admin [sn_grc_reg_change.admin] | The RCM Admin has access to all the aspects of the Regulatory Change Management application. | • sn_grc_reg_change.it_admin<br>• sn_grc_reg_change.manager |
| RCM IT Admin [sn_grc_reg_change.it_admin] | The RCM IT Admin sets up the integrations with third-party regulatory intelligence | • connection_admin<br>• action_designer<br>• import_admin |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role titles and names | Description | Available roles |
|---|---|---|
| | providers. The RCM IT Admin troubleshoots issues, if any. | • credential_admin<br>• flow_designer<br>• oauth_admin<br>• sn_grc.developer<br>**Note:** The GRC User role (sn_grc.user) contains the GRC Business User role (sn_grc.business_user). For more information, see . |
| RCM Manager [sn_grc_reg_change.manager] | The RCM Manager assigns regulatory alerts and monitors regulatory change tasks and action tasks.<br>**Note:** A group titled as **RCM Managers** is added under**Groups** in the **User Administration** panel under the Regulatory Change Management application. The RCM Managers group reviews the regulatory tasks workflow, ensuring regulatory compliance. The users who belong to this group must have the sn_grc_reg_change.manager role. | sn_grc_reg_change.user |
| RCM User [sn_grc_reg_change.user] | The RCM User assesses the applicability of the alerts, initiates impact assessments, and completes the assigned regulatory change tasks and action tasks. | • sn_compliance.reader<br>• sn_risk.reader |

## Download and install Regulatory Change Management

Download the GRC: Regulatory Change Management application from the ServiceNow Store and run it in your ServiceNow instance.

### Before you begin

Role required: sn_grc_reg_change.manager, sn_grc_reg_change.it_admin, or sn_grc_reg_change.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Download the GRC: Regulatory Change Management application from the ServiceNow Store.
   Follow the instructions for Download a GRC application from the ServiceNow Store for the first time. Downloading the Regulatory Change Management application automatically installs the following required applications:
   - GRC: Policy and Compliance Management
   - GRC: Advanced Risk
2. In your instance, navigate to **System Applications** > **All Available Applications** > **All**.
3. Locate GRC: Regulatory Change Management.
4. In the list, select an appropriate release.
5. Click **Install**.
   A new Application installation window is displayed.
6. Confirm the details of the application and click **Install**.

### Result

The GRC: Regulatory Change Management application is installed on your ServiceNow instance.

## Regulatory Change Management workflow

The workflow for the Regulatory Change Management application involves separate stages for installation, setup, and management.

The Regulatory Change Management application workflow goes through the following stages. These stages help you to manage regulatory changes:

1. Prerequisites: Ensure that the following applications are installed:
   - ServiceNow® GRC: Policy and Compliance Management application
   - ServiceNow® Advanced Risk application
2. Download and install the GRC: Regulatory Change Management application from the ServiceNow Store. For details, see Download and install Regulatory Change Management.
3. Assign roles to the users as needed. For details, see User roles in Regulatory Change Management.
4. To set up the Regulatory Change Management application, complete the following steps:
   - Create and validate the connections and credentials. For details, see Establish an SFTP or REST API connection.
   - Activate the integration flows. For details, see GRC integration with Thomson Reuters Regulatory Intelligence and Set up the RSS feeds.
   - Create and map the internal regulatory taxonomy. For details, see Map the taxonomy.
5. To manage the workflow, complete the following steps:
   - Assign the regulatory alerts. For details, see Manage and assign regulatory event alerts.
   - Assess the impact of the alerts and create regulatory change tasks. For details, see Manage the regulatory change tasks.
   - Evaluate the action tasks. For details, see Action tasks in Regulatory Change Management.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Implement the changes and create action tasks. For details, see Create an action task.
- Create and view issues related to regulatory tasks. For details, see Create an issue related to the regulatory tasks

6. Provide an overview of the regulatory changes via dashboards and reports. For details, see Regulatory Change Management dashboard.
7. Ensure an overall regulatory compliance for your organization.

## Process flow and tasks performed by different users

The Regulatory Change Management process flow consists of the tasks that are performed by different user roles for the regulatory change compliance.

Regulatory alerts are sourced from the external providers that provide data in the form of regulatory alerts. The alert may be received in the form of RSS feeds or from an external provider such as Thomson Reuters. The Regulatory Change Management application receives the new regulatory changes that are applicable to an organization.

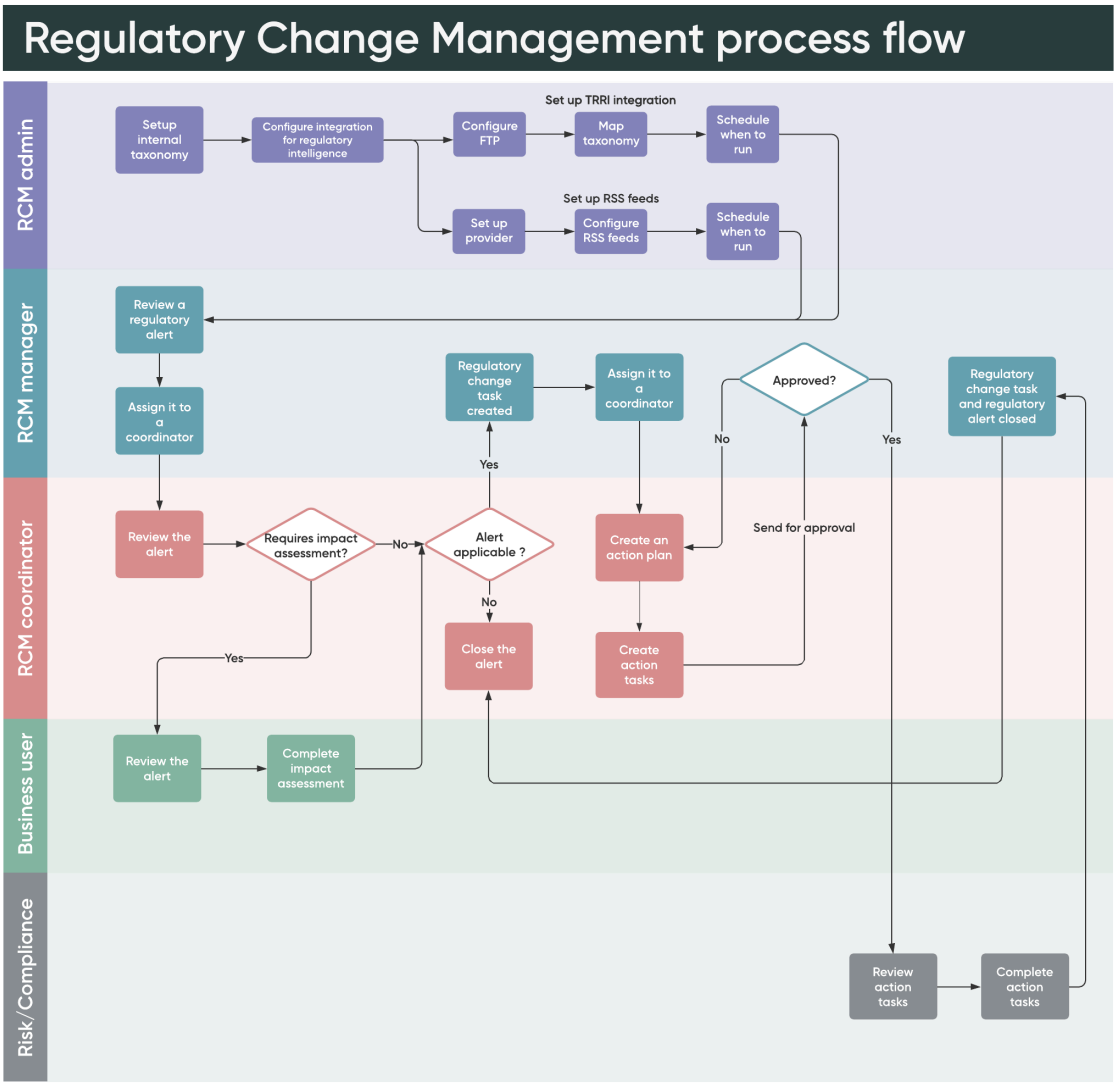
Similar to most of the IRM applications, the RCM application has the following user roles:

- RCM administrator: The administrator with the sn_grc_reg_change.admin user role.
- RCM Manager: The application manager with the sn_grc_reg_change.manager user role.
- RCM User or coordinator: The user with the sn_grc_reg_change.user user role. The person who is responsible for ensuring that the regulatory changes are assigned to the right teams and they are completed in time.
- Business user role: A user with the sn_grc.business_user role.
- Risk or Compliance manager: A user with sn_risk.manager or sn_compliance.manager role who would be performing the changes as part of the Regulatory Change Management application.

See the Regulatory Change Management process flow for reference.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Regulatory Change Management process flow and tasks performed by different users




Steps to complete the Regulatory Change Management process flow are listed in this section:

1. Set up the integration: Customers can subscribe to a public RSS feed for the regulatory bodies or they can also subscribe to a subscription provider such as Thomson Reuters Regulatory Intelligence (TRRI) that is a curated intelligence provider. Providers such as Thomson Reuters Regulatory Intelligence (TRRI) aggregate the regulatory changes from different sources and provide the collective changes in the form of feeds.
2. Set up the taxonomy: Taxonomy elements are different classifiers that an organization can apply to its reg content to categorize it. Taxonomy elements are used to create a hierarchical structure of different classifications for setting up the regulatory content for an organization. This is the process of setting up an internal taxonomy.
3. Review a regulatory alert: A user with the sn_grc_reg_change.manager role (RCM Manager) reviews a regulatory alert and assigns it to a coordinator or a user with the sn_grc_reg_change.user role (RCM User). The user with the sn_grc_reg_change.user role reviews the alert. If the regulatory change requires an impact assessment, the RCM user sends it to a subject matter expert (SME) with a business user role.
4. Assess the impact: The subject matter expert (SME) with a business user role assesses the impact of the regulatory change and sends the score of the impact assessment to

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the Regulatory Change Management application. If the alert is not applicable to the organization, the RCM user closes the alert. If the alert is applicable to the organization, the RCM user creates a new regulatory change task and assigns it to the same or a new coordinator.

5. Devise an action plan: The coordinator identifies the steps to comply with the regulatory change, devises an action plan, and creates the action tasks for different teams to complete the action items that have been identified. The coordinator further creates the action tasks associated with the regulatory change task. Once the action plan is created, it is sent to the RCM manager for an approval. The managers review the action plan and confirm if all the action tasks that have been created are enough or if some of the action tasks are not necessary.
6. Complete the action tasks: If the action plan is rejected, then the same coordinators again go through the action plan, update the actual tasks, and then the action plan is sent back for an approval. All Compliance based action tasks are visible to the Compliance Manager and Risk Managers can see the Risk based action tasks. Once the tasks are assigned to the Risk and Compliance users, the action tasks are tracked through completion. A due date is marked and tracked for the action tasks. Once the actual tasks are completed, the regulatory alert and the parent regulatory change task are closed.

   This step indicates completion of the regulatory change process flow.

## Setup checklist for Regulatory Change Management

Complete the tasks that are required to set up the Regulatory Change Management application. When you have completed these tasks, the base system is ready for operation. Optional setup procedures are also included to enhance Regulatory Change Management functionality.

### Before you begin

Role required: sn_grc_reg_change.admin

Consider creating and printing a PDF of this checklist topic. You can then check off tasks as you complete them. To generate a PDF, click the **Save As PDF** icon ( ) at the top of the topic and click **Selected topic**.

### Procedure

1. Install the Regulatory Change Management (RCM) application from the Store.
   For information on the installation process, see Download and install Regulatory Change Management.
2. Assign RCM roles to the users.
   For information on the roles, see User roles in Regulatory Change Management.
3. To set up the feeds, choose one of the following options.

| Step | Description |
|---|---|
| Set up the RSS feeds by using the RCM application. | For information on setting up the RSS feeds by using the RCM application, see Set up the RSS feeds. |
| Set up the feeds by integrating with the **GRC integration with Thomson Reuters Regulatory Intelligence** application. | For more information on setting up third-party integration with the RCM application, see GRC integration with Thomson Reuters Regulatory Intelligence. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Create and validate the connections and credentials.
   For more information, see Establish an SFTP or REST API connection.
5. Activate the integration flows.
   For more information, see GRC integration with Thomson Reuters Regulatory Intelligence and Set up the RSS feeds.
6. Create an internal regulatory taxonomy and map the taxonomy.
   For more information, see Map the taxonomy.
7. Assign regulatory feeds.
   For more information, see Manage and assign regulatory event alerts.
8. Assess the impact and assign related regulatory tasks.
   For more information, see Manage the regulatory change tasks.
9. Prepare an action plan to identify the changes that must be done.
   For more information, see Action tasks in Regulatory Change Management.
10. Create action tasks to implement the identified changes, and complete them.
    For more information, see Create an action task.
11. Provide an overview of the regulatory changes via dashboards and reports.
    For more information, see Regulatory Change Management dashboard.

## Regulatory Change Management application in the Compliance Workspace

Starting with GRC: Regulatory Change Management, version 13.0.1, the Regulatory Change Management application is available in the Compliance Workspace.

### Highlights of the Regulatory Change Management application in the Compliance Workspace

The Workspace provides a single-pane view with a personalized experience and simplified user journey for the users.

- Default home page for the Regulatory Change Management manager displays actionable insights and quick links.
- Contextual side panel displays the regulatory taxonomy for each regulatory alert record.
- Record pages provide holistic view with a quick summary and insights specific to what is being viewed.
- Form layout, field labels, messages, and breadcrumb navigation provide a consistent experience to the users across the ServiceNow® platform.
- 360° view provides an overview of data relationship for a record across an enterprise.

### Regulatory Change Management application views in the Compliance Workspace

The Regulatory Change Management application in the Compliance Workspace contains the following views for the users.

Home page view

Provides an overview of the Compliance posture of your organization.

Regulatory Change Management application landing page view

Provides an overview, trends, and tracking status of the regulatory activity across your organization.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Tasks view

Provides an overview of the tasks assigned to the users, user groups, reported items, and watchlist.

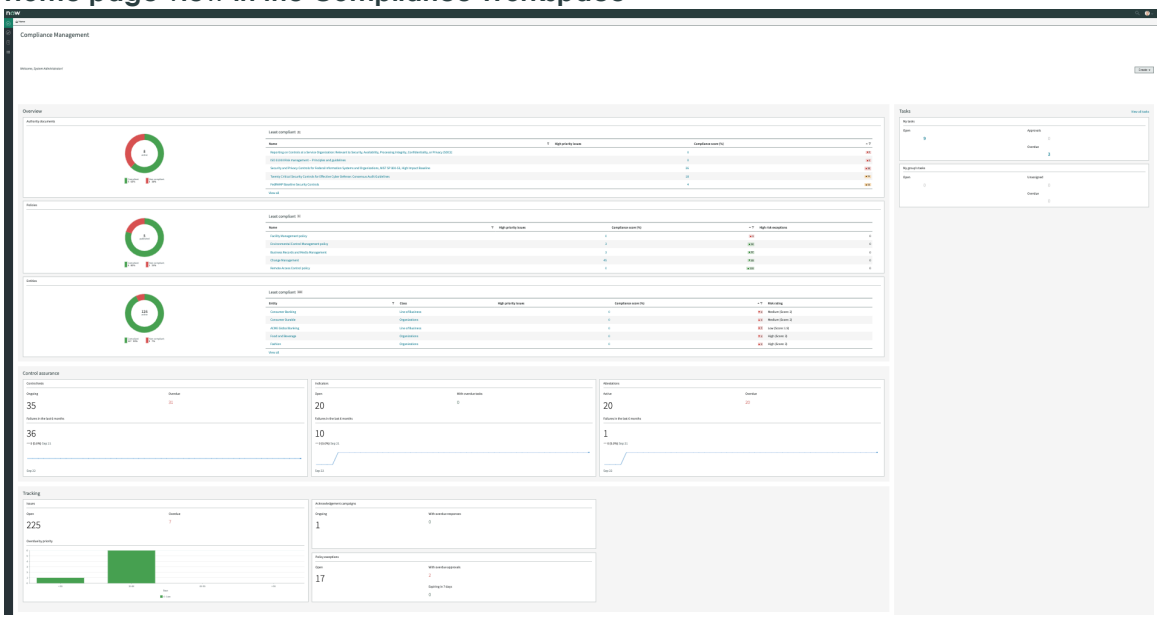
Issues overview landing page view

Provides an overview, tracking status, and performance trends of the issues.

List view

Provides the list of the GRC objects in the Compliance Workspace.

**Home page view in the Compliance Workspace**




**Note:** GRC administrators configure the tasks and issues in the Landing Page Configurations module in the classic user interface. These tasks and issues are visible to the end users in the landing pages of various workspaces. See Landing Page Configurations module for more information.

## Regulatory Change Management application landing page

The Regulatory Change Management application landing page view provides the overview of the regulatory activities in your organization. Users with the sn_grc_reg_change.manager roles only can view the Regulatory Change Management landing page in the primary navigation in the Compliance Workspace.

The prerequisites for displaying the Regulatory Change Management landing page in the Compliance Workspace are:

- Download the GRC: Regulatory Change Management application from the ServiceNow Store in your instance.
- Log in as a user with the sn_grc_reg_change.manager role into the Regulatory Change Management application.

The Regulatory Change Management application managers with the sn_grc_reg_change.manager user role assign the regulatory alerts and monitor the associated regulatory change tasks, import document tasks, and action tasks.

The Regulatory Change Management application in the Compliance Workspace is designed for the users with the following roles:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Regulatory Change Management application managers with the sn_grc_reg_change.manager role: Only the users with the sn_grc_reg_change.manager role can view the Home page of the Regulatory Change Management application in the Compliance Workspace.
- Regulatory Change Management application users with the sn_grc_reg_change.user role: Users with the sn_grc_reg_change.user role can view the tasks assigned to them in the Regulatory Change Management application, but they cannot view the Regulatory Change Management application landing page in the Compliance Workspace.

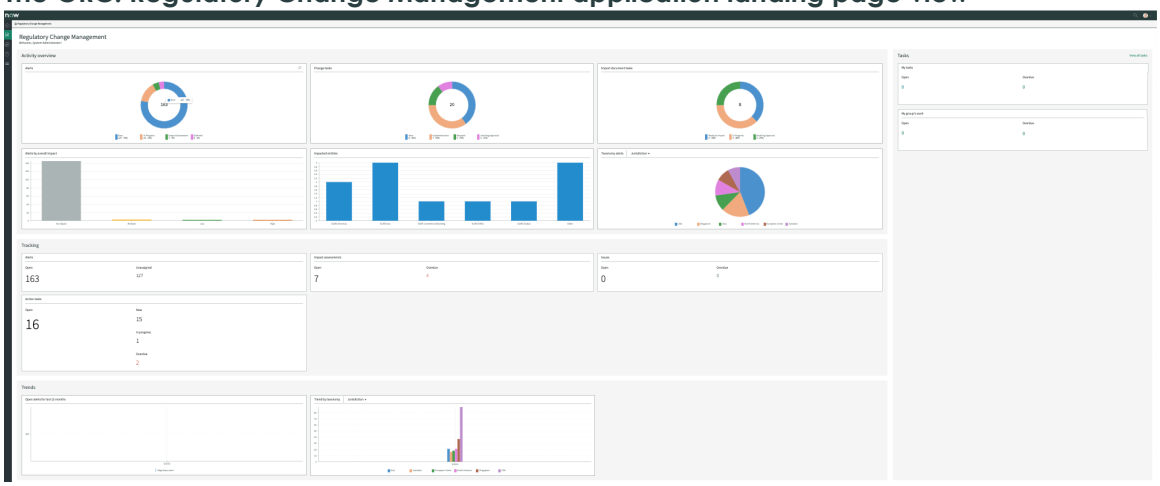
## Landing page view

The landing page view consists of the data visualization widgets that display the regulatory activity across your organization. The data visualization widgets are clickable widgets that use color coding to distinguish the states of the alerts and the tasks. You can click each widget to view all the associated regulatory alerts or tasks. The color scheme for each donut chart or bar graph is displayed in each subsection.

The GRC: Regulatory Change Management landing page displays the following sections:

- Activity overview
- Trends
- Tracking
- Tasks

**The GRC: Regulatory Change Management application landing page view**




- Activity overview: This section contains an overview of the regulatory alerts and the tasks associated with the regulatory alerts across your organization.

**Activity overview**

| Section | Description |
|---|---|
| Alerts | Active regulatory alerts that are new, in progress, and deferred in numbers and percentage displayed in a donut chart. Also displays impact assessment tasks associated with the alerts. |
| Change tasks | Active change tasks that are in new, implementation, respond, and awaiting approval state displayed in a donut chart. The tasks are displayed in numbers and the percentage. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Section | Description |
|---|---|
| Import document tasks | Active import document tasks that are in ready to import, in progress, and awaiting approval state displayed in a donut chart. The tasks are displayed in numbers and the percentage. |
| Alerts by overall impact | Displays the overall impact of the regulatory alerts such as no impact, low, medium, and high impact alerts displayed in a bar graph. |
| Impacted entities/ Business lines impacted | Grouping of the impact assessment reports based on the impacted entities in a bar graph. The bar graph displays a maximum of five entities for a better display. |
| Taxonomy alerts | Taxonomy alerts as per the taxonomy elements such as content type, jurisdiction, regulatory body, sector, and theme. |

- Trends: This section displays the trends for the open alerts or trends by the taxonomy elements.

**Trends**

| Section | Description |
|---|---|
| Open alerts for last 12 months | Timeline of the incoming regulatory alerts that are active and are not closed over a period of 12 months. For example, if 10 records are received every month, they are grouped by a quarter and a total of 30 records for each quarter are displayed in the line graph. Four plots are displayed on the X-axis and 30 records are displayed in each plot. |
| Trends by taxonomy | Trends noted by the taxonomy elements such as content type, jurisdiction, regulatory body, sector, and theme. |

- Tracking: This section displays the tracking status of the regulatory alerts and the associated regulatory tasks.

**Tracking**

| Section | Description |
|---|---|
| Alerts | Tracking status of the regulatory alerts such as open and unassigned alerts. |
| Impact assessments | Status of the impact assessments such as open and unassigned impact assessments. |
| Issues | Status of the issues such as open and overdue issues. |
| Action tasks | Active action tasks that are open including the action tasks that are in new, in progress, and overdue states. |

- Tasks: This section contains an overview of the user's tasks and user group's tasks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tasks**

| Section | Description |
|---|---|
| My tasks | Tasks assigned to the user such as open and overdue tasks. |
| My group's work | Tasks assigned to the user group such as open and overdue tasks. |
| View all tasks | Link to the Tasks view in the Home page. |

## Regulatory alerts

The List view in the Regulatory Change Management application in the Compliance Workspace displays all the regulatory alerts received under the **Regulatory alerts** option in the menu. The **Unassigned alerts** list displays all the new and unassigned regulatory alerts. The Type column in the **Unassigned alerts** list displays the type of the regulatory alert.

The regulatory alerts are of two types:

- Regulatory event alert
- Source document alert

When you click the title of a regulatory event alert or a source document alert in the List view, it displays the details of the alert in a new page.

The regulatory event alerts page displays the following tabs and related lists by default:

- Overview tab
- Details tab
- Related documents list
- Impact assessments list

The source document alerts page displays the following tabs by default:

- Overview tab
- Details tab

## Regulatory event alerts view

When you click a regulatory event alert in the List view in the Compliance Workspace, it displays the details of the alert on a new page. The details include the title of the alert, provider of the alert, its state, and other important information in the Overview tab and Details tab.

The regulatory event alerts page also displays the following tabs and related lists associated with the alert:

- Overview tab
- Details tab
- Related documents list
- Impact assessments list

The following section provides more information on the tabs and the related lists that are associated with the alert.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Overview tab

| Field | Description |
|---|---|
| Description | Detailed description of the regulatory event alert. |
| Stage: Stepper component for regulatory event alert | Stepper component for the regulatory event alert that displays the following stages:<br>• New: When a regulatory event alert is marked as applicable, the state of the alert is updated automatically to **In progress** in the Stepper component and a regulatory change task is automatically created.<br>• Impact Assessment: When an impact assessment is initiated on the regulatory event alert, the stage in the stepper component is updated automatically to **Impact Assessment**.<br>• In progress: When the state of the regulatory event alert is updated to**In progress**, the highlighted stage in the stepper component is displayed as **In progress**.<br>• Closed: When the Regulatory event alert is in **Closed** state, the highlighted stage in the stepper component is displayed as **Closed**. |

### Details tab

| Field | Description |
|---|---|
| Regulatory alert | Details of the alert such as title of the alert, citation associated with the alert, provider URL, regulatory body URL, name of the provider, type of the alert, and coordinator of the alert. |
| Dates | Details of the important dates associated with the alert such as source publication date, comments date, effective date, compliance date, and expiration date. |
| Compose additional comments | Text box for entering additional comments related to the activity. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

#### Related Documents list

| Field | Description |
|---|---|
| Related documents | Details of the related documents associated with the alert such as citation, citation reference, title, and type. |

#### Impact assessments related list

| Field | Description |
|---|---|
| Impact assessments | Details about the impact assessment of the alert such as entity, risk assessment, assessor, inherent risk, and state. |

Taxonomy side-panel: The taxonomy side-panel displays the following taxonomy classes for the Regulatory event alert:

- Regulatory bodies
- Content types
- Jurisdictions
- Themes
- Sectors

**Note:** The taxonomy classes are displayed only if the records have any values associated with them. For example, if the regulatory alert does not have any values for the taxonomy class Jurisdictions, the taxonomy category Jurisdictions is not displayed in the taxonomy side panel.

## Source document alerts view

When you click a source document alert in the List view in the Compliance Workspace, it displays the details of the alert on a new page. The details include the title of the alert, provider of the alert, its state, and other important information in the Overview tab and Details tab.

The source document alerts page also displays the following tabs:

- Overview tab
- Details tab

See more information on the tabs.

#### Overview tab

| Field | Description |
|---|---|
| Citation | Citation associated with the source document alert. |
| Stepper component | Process flow stepper component for the source document alert that displays the following stages: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Overview tab (continued)

| Field | Description |
|---|---|
| | • New: When the source document type alert is in the **New** state, the highlighted stage in the stepper component is displayed as **New**.<br>• In progress: When the state of the source document type alert is updated to **In progress**, the highlighted stage in the stepper component is displayed as **In progress**.<br>• Closed: When the source document type alert is in **Closed** state, the highlighted stage in the stepper component is displayed as **Closed**. |

### Details tab

| Field | Description |
|---|---|
| Regulatory alert | Details of the alert such as title of the alert, citation associated with the alert, provider URL, regulatory body URL, name of the provider, type of the alert, and coordinator of the alert. |
| Dates | Details of the important dates associated with the alert such as source publication date, comments date, effective date, compliance date, and expiration date. |
| Activity journal | Text box for entering additional comments related to the alert. |
| Compose additional comments | Text box for entering additional comments related to the activity. |

Taxonomy side-panel: The Taxonomy side-panel displays the following taxonomy details for the source document type alerts:

- Regulatory bodies
- Content types
- Jurisdictions
- Themes
- Sectors

**Note:** The taxonomy classes are displayed only if the records have any values. For example, if the regulatory alert does not have any values for the taxonomy class Jurisdictions, the taxonomy category Jurisdictions is not displayed in the taxonomy side panel.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Regulatory tasks in Compliance Workspace

You can perform various regulatory tasks in the Regulatory Change Management application in Compliance Workspace and receive granular information on the tasks and alerts using the data visualization widgets.

The Regulatory Change Management workflow and the Regulatory Change Management process flow provide information on the regulatory tasks that are performed by the Regulatory Change Management application users to comply with the regulatory changes. See the Regulatory Change Management workflow and Process flow and tasks performed by different users for more information.

You can perform the following GRC: Regulatory Change Management configuration tasks in Compliance Workspace:

- Assign the regulatory event alert to a Coordinator. For more information, see Assign the regulatory event alert to a coordinator.
- Assess the impact of the regulatory event alert, complete the assessment, and manage the regulatory change tasks associated with the alert. For more information, see Assess the impact of a regulatory event alert and Manage the regulatory change tasks.
- Assign the source document alert to a Coordinator. For more information, see Assign the source document alert to a coordinator.
- Manage the source document import tasks associated with the source document alert. For more information, see Manage the source document import task.
- Manage the action tasks that are associated with the regulatory event alerts and the source document alerts. For more information, see Create a new action task for the alert and Complete the action task associated with the alert.
- Create an issue related to a regulatory task. For more information, see Create or add an issue related to a regulatory task.
- Map the taxonomy. For more information, see Manage the taxonomy.

### Assign the regulatory event alert to a coordinator

Log in to the GRC: Regulatory Change Management application, review the regulatory event alert, update the details, and assign it to a coordinator.

#### Before you begin

Role required: sn_grc_reg_change.manager, sn_grc_reg_change.user

#### About this task

In the following procedure, step 4 and after describe various actions that users with the sn_grc_reg_change.manager role or sn_grc_reg_change.user role can perform.

#### Procedure

1. Log in with the sn_grc_reg_change.manager user role.
2. Navigate to **All** > **Regulatory Change Management** > **Compliance Workspace**.
   The Regulatory Change Management application in the Compliance Workspace is displayed.
3. Navigate to **Lists** > **Assigned Regulatory Alerts** view.
4. In the Assigned Alerts list, select a regulatory event alert.
   The detailed view for the selected regulatory event alert is displayed.
5. In the Details tab, fill in the form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Details tab

| Fields | Description |
|---|---|
| Title | Title of the alert as received from the provider. This field is automatically set to display the title. |
| Description | Description and a summary of the event. This field is automatically set to display the description. |
| Provider URL | URL of the alert that is received from the provider. This field is automatically set to display the provider URL. |
| Regulatory body URL | URL of the regulatory body that is associated with the alert. This field is automatically set to display the regulatory body URL. |
| Provider | Name of the alert provider. This field is automatically set to display the name of the alert provider. |
| Type | Type of regulatory alert. This field is automatically set to display the type of the alert. |
| Coordinator | User that the alert is assigned to. |
| Overall impact | Overall impact of the alert. |
| Dates | |
| Source publication date | Date when the regulatory event is published by the regulatory body. This field is automatically set to display the source publication date. |
| Comments date | Date until when the comments can be provided for the regulatory event. This field is automatically set to display the comments date. |
| Effective date | Date when the regulatory event is going to be applicable. This field is automatically set to display the effective date. |
| Compliance date | Date by which the regulatory event is going to be compliant. This field is automatically set to display the compliance date. |
| Expiration date | Expiry date for the regulatory event. This field is automatically set to display the expiration date. |
| Series data | |
| Series name | Series name of the alert. This field is automatically set to display the series name from the provider. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Fields | Description |
|---|---|
| Sequence number | Sequence number of the alert. This field is automatically set to display the sequence number from the provider. |
| Activity Journal | |
| Additional comments | Additional comments related to the alert. |
| Compose | |
| Compose section | Additional comments related to the alert. |
| Activities | Log of the activities related to the alert. |
| Highlighted details | |
| Taxonomy | Taxonomy details associated with the alert. This field is automatically set to display the taxonomy details of the alert. |

**Note:** Beginning with the ServiceNow® Utah release, the taxonomy section in the form is not available to the new installations.

6. In the **Coordinator** field, assign the regulatory event alert to a coordinator with the sn_grc_reg_change.user user role and click **Save**.

### Result
The regulatory event alert is assigned to the selected coordinator.

### What to do next
Assess the impact of a regulatory event alert

#### Assess the impact of a regulatory event alert

Assess the impact of a regulatory event alert by creating an assessment on the regulatory event alert. Assign the impact assessment to the owner of the business entity that is affected by the alert.

### Before you begin
Role required: sn_grc_reg_change.user

### About this task
As a user with the sn_grc_reg_change.user role, you can review the regulatory event alert and initiate an impact assessment on the alert.

### Procedure

1. Log in with the sn_grc_reg_change.user role.
2. Navigate to **All** > **Regulatory Change Management** > **Compliance Workspace**.
   The Regulatory Change Management application in the Compliance Workspace is displayed.
3. Navigate to **Lists** > **Assigned Regulatory Alerts** view.
4. Select the regulatory event type alert that is assigned to you as the coordinator of the alert.
5. Click **Initiate Impact Assessment**.
6. Select any entity from the Entities list for the impact assessment and click **Create Assessments**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** Perform an impact assessment on the regulatory event alert in the classic user interface as the form is not yet migrated to the Workspace. For more information, see Assess the impact of a regulatory change.

If no entities are configured, you can configure new entities. See Configure an entity class for more information.

### Result

In the Impact assessments related list, the new impact assessment is listed and it is automatically assigned to the entity owner. The entity owner reviews it and sends feedback on the assessment. After completing the assessment, the calculated inherent risk is displayed under the **Assessment Summary** tab. When the entity owner clicks **Mark as complete** on the impact assessment, it saves the assessment details and marks it as Complete.

### What to do next

See Manage the regulatory change tasks for information on marking the alert as applicable and managing the regulatory change tasks.

## Manage the regulatory change tasks

Manage the regulatory change tasks that are associated with the regulatory event alert. When a business entity owner completes the impact assessment on the regulatory event alert, the user with the sn_grc_reg_change.user role reviews the assessment summary and marks the alert as applicable.

### Before you begin

Role required: sn_grc_reg_change.manager, sn_grc_reg_change.user

### About this task

The coordinator of the regulatory event alert identifies the steps to comply with the regulatory change and manages the regulatory change task.

### Procedure

1. Navigate to **All** > **Regulatory Change Management application** > **Compliance Workspace**. The Regulatory Change Management application in the Compliance Workspace is displayed.
2. Navigate to **Lists** > **Regulatory Alerts** view.
3. Select the regulatory event alert for which a business entity owner has completed the assessment.
4. Review the impact assessment and mark the alert using one of the following options.

| Field | Description |
|---|---|
| Applicable | Mark the alert as applicable. After marking the regulatory event alert as **Applicable**, a new regulatory change task is automatically created in the Regulatory Tasks related list in the regulatory alert UI page. |
| Not applicable | Mark the alert as not applicable.<br><br>When you mark the alert as not applicable, a message window displays. Select one of the following reasons in the **Reasons** list and click **Submit**: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ No action required on the alert<br>◦ Duplicate alert<br>◦ Other<br>As a result of this action, the stepper component displays the alert stage as **Completed**. |
| Cancel regulatory alert | Cancel the regulatory alert. |
| Defer | Defer the alert to a later date. |

5. For the applicable alert, click the **Regulatory Tasks** related list and click the regulatory change task that is created for the alert.
6. In the Details tab, fill in the form.

**Regulatory Change Task form**

| Field | Description |
|---|---|
| Regulatory Change Task | |
| Regulatory alert | Title of the regulatory alert associated with the source document import task. This field is automatically set to display the title of the alert. |
| Instructions | Instructions related to the source document import task. |
| Assignment | |
| Assignment group | Assignment group for the record. The group is selected from the **Group Hierarchy** table. |
| Approver type | Approver type for the task. Choices are as follows:<br>◦ **User**<br>◦ **Group** |
| Assigned to | User to which the task is assigned. |
| Approver or Approver group | If the approver type is a group, the **Approver group** field is displayed.<br>If the approver type is a user, the **Approver** field is displayed. |
| Schedule | |
| Due date | Due date for the source document import task. |
| Approved on | Date when the source document import task is approved. This field is automatically set to display the approval date. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Activity Journal | |
| Watchlist | Users that are in the watchlist for this task. |
| Work notes list | Users that are in the work notes for this task. |
| Work notes (Private) | Work notes related to the task. |
| Compose | |
| Worknotes | Worknotes typed in by the users. These work notes can be posted for reference. |
| Activity | |
| Activity | Activity and state of the task. |
| Attachments | |
| Attachments | Attachments related to the task. |

7. Verify that the mandatory fields such as **Approver**, **Assigned to**, and **Due date** are updated.
8. Click **Respond**.
   The **Respond** action triggers the impact radius calculation in the background. For information on impact radius calculation, see Impact radius calculation and approval. The regulatory change task is updated with the **Responded** state.
9. Add an action task if necessary.
   See Create a new action task for the alert for creating an action task.
10. Add issues if necessary.
    See Create or add an issue related to a regulatory task for more information.
11. After creating necessary action tasks and issues, click **Request Approval**.
    Depending on the state of the approval, the action task is activated. When the action task is closed, the associated source document import task is automatically closed.

### Result
Verify that the regulatory change task is updated with the **Responded** state and the Action tasks related list is displayed for the regulatory event alert.

### What to do next
Create a new action task for the alert

#### Assign the source document alert to a coordinator

Log in to the GRC: Regulatory Change Management application, review the source document alert, and assign it to a coordinator. The coordinator then assesses the applicability of the alert and completes the associated regulatory tasks.

### Before you begin
Roles required: sn_grc_reg_change.manager, sn_grc_reg_change.user

### About this task
As a manager, you can view and assign the source document alerts to users with the sn_grc_reg_change.user role. The user can then perform actions on the source document alerts.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Log in with the sn_grc_reg_change.manager user role.
2. Navigate to **All** > **Regulatory Change Management** > **Compliance Workspace**.
   The Regulatory Change Management application in the Compliance Workspace is displayed.
3. Navigate to **Lists** > **Assigned Regulatory Alerts** view.
4. Select a source document type alert in the list.
5. In the Details tab, fill in the form.

**Details tab in the Source Document alert form**

| Fields | Description |
|---|---|
| Title | Title of the source document type of alert as received from the provider. This field is automatically set to display the title. |
| Citation | Citation number for the source document that is received from the provider. This field is automatically set to display the citation. |
| Provider URL | URL of the alert provider. This field is automatically set to display the provider URL. |
| Regulatory body URL | URL of the regulatory body that is associated with the alert. This field is automatically set to display the regulatory body URL. |
| Provider | Name of the alert provider. This field is automatically set to display the name of the provider. |
| Type | Type of the regulatory alert. For example, source document alert. This field is automatically set to display the type of the alert. |
| Coordinator | User that the alert is assigned to. |
| Dates | |
| Source publication date | Date when an alert is published by the regulatory body. Auto-populated field. This field is automatically set to display the source publication date. |
| Comments date | Date until when the comments can be provided for the alert. Auto-populated field. This field is automatically set to display the comments date. |
| Effective date | Date when the alert is going to be applicable. This field is automatically set to display the effective date. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Fields | Description |
|---|---|
| Compliance date | Date by which the alert is going to be compliant. This field is automatically set to display the compliance date. |
| Expiration date | Expiry date for the alert. This field is automatically set to display the expiration date. |
| Activity Journal | |
| Additional comments | Additional comments related to the alert. |
| Compose | |
| Additional comments | Additional comments related to the alert that are added in the Compose section. |
| Log of the activities | Log of the activities related to the alert. Displays the system generated changes and additional comments. |
| Highlighted details | |
| Taxonomy | Taxonomy details associated with the alert. This field is automatically set to display the taxonomy details of the alert. |

6. In the **Coordinator** field, assign it to a user with the sn_grc_reg_change.user user role.
7. Log in with the sn_grc_reg_change.manager role, open the selected source document alert, and mark the alert using one of the following options.

| Field | Description |
|---|---|
| Applicable | Marks the alert as applicable. |
| Not applicable | Marks the alert as not applicable. Select one of the following reasons and click **Submit**:<br>◦ No action required on the alert<br>◦ Duplicate alert<br>◦ Other<br>As a result of this action, the stepper component in the alert page displays the stage as **Completed**. |
| Cancel regulatory alert | Cancel the regulatory alert. |
| Defer | Defer the alert to a later date. |

**Result**

After marking the source document alert as **Applicable**, a new source document import task is created under the Import document tasks related list.

**What to do next**

Manage the source document import task

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Manage the source document import task

Manage the source document import tasks that are associated with the source document alerts. When a source document alert is marked as applicable, a source import document task is created automatically.

## Before you begin

Role required: sn_grc_reg_change.manager, sn_grc_reg_change.user

## About this task

A source document import task is used to ingest a particular source document that is received from the provider into the regulatory library.

## Procedure

1. Navigate to **All** > **Regulatory Change Management application** > **Compliance Workspace**. The Regulatory Change Management application in the Compliance Workspace is displayed.
2. Navigate to **Lists** > **Regulatory Alerts** view.
3. Select the source document alert that you assessed previously and click the import document task.
4. In the Details tab, fill in the form.

**Source document import task form**

| Field | Description |
|---|---|
| Import Document Task | |
| Regulatory alert | Title of the regulatory alert associated with the import document task. This field is automatically set to display the alert title. |
| Instructions | Instructions related to the import document task. |
| Assignment | |
| Assignment group | Assignment group for the record. The group is selected from the **Group Hierarchy** table. |
| Approver type | Approver type for the task. Choices are as follows:<br>◦ **User**<br>◦ **Group** |
| Assigned to | User to which the task is assigned. |
| Approver or Approver group | If the approver type is a group, the **Approver group** field is displayed.<br>If the approver type is a user, the **Approver** field is displayed. |
| Schedule | |
| Due date | Due date for the source document import task. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Approved on | Date when the source document import task is approved. This field is automatically set to display the approval date. |
| Activity Journal | |
| Watchlist | Users that are in the watchlist for this task. |
| Work notes list | Users that are in the work notes for this task. |
| Work notes (Private) | Work notes related to the task. |
| Compose | |
| Worknotes | Worknotes typed in by the users. These work notes can be posted for reference. |
| Activity | |
| Activity | Shows the activity and state of the task. Auto-populated field. |
| Attachments | |
| Attachments | Attachments related to the task. |

5. Verify that the **Assigned to**, **Approver**, and **Due date** fields are updated.
6. To save the changes, click **Save**.
7. To update the selected source document import task, click **Work in progress**.
8. Navigate to the Action tasks related list and add an action task if necessary.
   See Create a new action task for the alert for creating a new action task.
9. Navigate to the Issues related list and add an issue if necessary.
   See Create or add an issue related to a regulatory task for adding an issue.
10. In the Import Task section, insert a new citation or update an existing citation as described in the table.

| Field | Description |
|---|---|
| Insert action | Action associated with the citation. Click **Insert** to insert a new citation.<br>**Note:** The **Insert** or **Update** action related to the citation is available only when the source document import task is in the **In progress** state. |
| Create under an existing Authority Document or Citation | Option to create a new citation under an existing authority document or citation. When this option is selected, a child authority document or a child citation is created under an existing citation. This option is displayed only when the **Insert** action is selected. |
| Parent type | Parent authority document or citation. This field is displayed only when the **Create un-** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **der an existing Authority Document or Citation** option is enabled. |
| Parent authority document | Parent authority document or citation from the library. This field is displayed only when the **Create under an existing Authority Document or Citation** option is enabled. |
| Update action | Action associated with the citation. Click **Update** and add the citation in the **Target citation** field to update an existing citation. |

11. Click **Request Approval**.

### Result
The state of the source document import task is updated to **Awaiting Approval**. Depending on the state of the approval, the action task is activated.

### What to do next
See Create a new action task for the alert and Complete the action task associated with the alert for information on creating a new action task and completing an action task associated with the alert.

#### Create a new action task for the alert

Create a new action task for the alert so that you can assign the action tasks to the compliance and risk users and mark a due date for the action tasks.

### Before you begin
Role required: sn_grc_reg_change.user

### About this task
The user with the sn_grc_reg_change.user role assigns the selected action task to the users with the sn_compliance.manager and sn_risk.manager roles depending on the action area of the alert such as compliance or risk. Once the compliance and risk users complete the action tasks associated with the alert, the alert and the parent regulatory change task are closed automatically.

### Procedure
1. Navigate to **All** > **Regulatory Change Management** > **Compliance Workspace**.
   The Regulatory Change Management application in the Compliance Workspace is displayed.
2. In the List view, navigate to **Lists** > **Regulatory Alerts** > **Assigned Alerts** view.
3. Complete one of the following tasks depending on the type of the alert.

| Field | Description |
|---|---|
| Regulatory event alert | Select the regulatory event alert for which the regulatory change task is in the **In progress** state and the Action tasks related list is displayed in the alert UI page. |
| Source document alert | Select the source document alert for which the source document import task is in the **In** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **progress** state and the Action tasks related list is displayed in the alert UI page. |

4. Navigate to the Action Tasks related list and click **New**.

**Note:** Only when the regulatory task is in **Respond** state, you can create a new action task.

**Action tasks form**

| Field | Description |
|---|---|
| Regulatory Task | Unique identification number for the regulatory task. This field is automatically set to display the regulatory task identification number. |
| Due date | Due date of the action task. This field is automatically set to display the due date. |
| Category: Compliance | |
| Compliance action target | Category type of the action task. When the selected category is **Compliance**, select the **Compliance action target** from the available options. Specific GRC object to be selected related to compliance such as authority document, citation from the list menu, and the associated document. |
| Category: Risk | |
| Risk action target | When the selected category is **Risk**, select the **Risk action target** from the available options. Specific GRC object to be selected related to risk such as risk statement. |
| Assignment | |
| Assignment Group | Group that is assigned the action task. This field is automatically set to display the assignment group. |
| Assigned to | User who is assigned the task. This field is automatically set to display the assignee of the task. |
| Priority | Priority of the action task such as planning, low, moderate, high, and critical. This field is automatically set to display the priority of the task. |
| Short description | Short description of the action task. |
| Instructions | Instructions related to the action task. |
| Activity Journal | |
| Watch list | List of users who receive notifications about the updates. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Work notes | Log of the work notes. |
| Worknotes list | List of the users who receive notifications about the work notes. |
| Attachments | |
| Attachments | Attachments related to the task. |

5. In the action tasks form, verify that the mandatory fields such as **Category**, **Compliance action target**, **Short description**, and **Instructions** are updated.
   The action task is marked for the sn_compliance.manager or the sn_risk.manager users.
6. To save the changes, click **Save**.

### Result
The action task is marked for the users with the sn_compliance.manager or the sn_risk.manager roles.

### What to do next
Complete the action task associated with the alert

#### Complete the action task associated with the alert

Complete the action tasks that are related to the regulatory event alerts and source document alerts. The compliance and risk users complete the action tasks that are assigned to them. The compliance and risk managers track the progress on the action tasks.

### Before you begin
Role required: sn_compliance.manager, sn_risk.manager, sn_compliance.user, sn_risk.user, sn_grc_reg_change.manager

### About this task
The action tasks are created as a follow-up to complete the changes that have been identified as part of the regulatory change tasks and source document import tasks. The actions described in the following steps are performed by the users with the sn_compliance.manager, sn_risk.manager, sn_compliance.user, sn_risk.user, and sn_grc_reg_change.manager roles.

### Procedure
1. Log in with the sn_compliance.manager or the sn_risk.manager user role.
2. Navigate to **All** > **Regulatory Change Management** > **Compliance Workspace**.
   The Regulatory Change Management application in the Compliance Workspace is displayed.
3. In the List view, navigate to **Lists** > **Regulatory Alerts** > **Assigned Alerts** view.
4. Navigate to the action task that is marked for you.
5. Assign the action task as described in the table.

| Role | Description |
|---|---|
| sn_compliance.manager | Log in with the sn_compliance.manager user role. Assign the action task associated with the regulatory event alert or the source document alert to the user with the sn_compliance.user role. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Role | Description |
| --- | --- |
| sn_risk.manager | Log in with the sn_risk.manager user role. Assign the action task associated with the regulatory event alert or the source document alert to the user with the sn_risk.user role. |

6. Complete the action task as described in the table.

| Role | Description |
| --- | --- |
| sn_compliance.user | Log in with the sn_compliance.manager user role. Complete the action tasks that are assigned to you and mark the state of the action task as **Completed**. |
| sn_risk.user | Log in with the sn_risk.manager user role. Complete the action tasks that are assigned to you and mark the state of the action task as **Completed**. |

7. Verify the status of the action task as described in the table.

| Role | Description |
| --- | --- |
| sn_compliance.manager | Log in with the sn_compliance.manager user role. Verify that the action task associated with the regulatory event alert or the source document alert has been completed by the user with the sn_compliance.user role. |
| sn_risk.manager | Log in with the sn_risk.manager user role. Verify that the action task associated with the regulatory event alert or the source document alert has been completed by the user with the sn_risk.user role. |

### Result

Once the user with the sn_compliance.user or the sn_risk.user role completes the action task, the regulatory event alert and the parent regulatory change task are closed automatically. Similarly, the source document alert and the parent source document import task are closed when the associated action tasks are completed. This is the final step of the regulatory tasks workflow.

## Create or add an issue related to a regulatory task

Create or add an issue related to a regulatory task to document the observations, changes in the citation, discrepancies, or to notify about any problems. You can also identify the source of the issue to analyze and classify the issues.

### Before you begin

Role required: sn_grc_reg_change.manager, sn_grc_reg_change.user

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Regulatory Change Management application** > **Compliance Workspace** > **Regulatory alert**.
   The Regulatory Change Management application in Compliance Workspace is displayed.
2. On the regulatory change task form, navigate to the **Issues** tab.

   You can add an existing issue to a regulatory task or create an issue that you can relate to a regulatory task.

| Step | Description |
|---|---|
| Select **Add**. | Relate a regulatory task to an existing issue. |
| Select **New**. | Create an issue that you can relate to a regulatory task. |

3. Click **Save**.

#### Create New Issue form

Use the Create New Issue form in Compliance Workspace to create an issue or add an existing issue to a regulatory task.

## Create New Issue form

For a description of the field values, see the following table.

**Create New Issue form**

| Field | Description |
|---|---|
| Issue | |
| Number | Number of the issue. This field is auto-filled. |
| Name | Name of the issue. |
| Issue source | Source of the issue, such as Business service or Scenario analysis. This field is auto-filled. |
| Issue type | Source from where the issue was created. This field is auto-populated with one of the following options based on how the issue is created:<br>• Control design effectiveness failure<br>• Control operative effectiveness failure<br>• Control does not meet requirement<br>• Control does not exist<br>• Non-compliance to a regulation<br>• Non-compliance to a policy<br>• Improvement or suggestion to an existing policy<br>• Recommendation for a new policy<br>• process optimization or improvement<br>• Observation<br>• Data breach |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| | • Fraud<br>• Misstatement<br>• Training<br>• Documentation |
| Classification | Classification of the issue. This field is auto-populated with one of the following options:<br>• Audit<br>• Compliance<br>• Operational Resilience<br>• Risk<br>• Vendor |
| Location | Location of the issue. |
| State | State of the issue. Available options are:<br>• New<br>• Analyze<br>• Respond<br>• Review<br>• Closed Complete<br>• Closed Incomplete |
| Substate | Substate of the issue. This field is auto-filled. |
| Priority | Priority of the issue. Available options are:<br>• Critical<br>• High<br>• Moderate<br>• Low<br>• Planning |
| Issue rating | Rating of the issue. Available options are:<br>• Very High<br>• High<br>• Moderate<br>• Low<br>• Very Low |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| Description | Approver of the scenario analysis plan. |
| Assignment | |
| Assignment group | Assignment group for the issue. For example, Application Development group. |
| Assigned to | User that the issue is assigned to. |
| Issue manager group | Manager group that the issue is assigned to. Available options are:<br>• Compliance Managers<br>• IT Risk Managers<br>• Risk Managers |
| Issue manager | Manager that the issue is assigned to. |
| Watchlist | Users who are on the watchlist for the issue. |
| Schedule | |
| Due date | Date when the issue is due. |
| Confirmed date | Confirmation date for the issue. This field is auto-filled. |
| Planned start date | Planned start date for the issue. |
| Planned end date | Planned end date for the issue. |
| Duration | Duration for the issue in days, hours, minutes, and seconds. |
| Created | Date on which the issue is created. This field is auto-filled. |
| Closed | Date on which the issue is closed. |
| Actual start date | Actual start date for the issue. |
| Actual end date | Actual end date for the issue. |
| Actual duration | Actual duration for the issue in days, hours, minutes, and seconds. |
| Issue grouping | |
| Parent issue | Parent issue that is associated with the issue. |
| Issue group rule | Group rule for the issue. This field is auto-filled. |
| Action plan | |
| Recommendation | Recommendation for the issue. |
| Action plan | Action plan for the issue. |
| Activity | |
| Work notes | Work notes for the issue. |
| Additional comments | Additional comments for the issue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create New Issue form (continued)**

| Field | Description |
|---|---|
| Settings | |
| Functional domain | Functional domain for the issue. |

### Manage the taxonomy

Manage the taxonomy when you are setting up the Regulatory Change Management application in the Compliance Workspace. Create an internal taxonomy and map the internal taxonomy to the external taxonomy so that the Regulatory Change Management application refers to only one taxonomy.

## Before you begin

Role required: sn_grc_reg_change.admin

## Procedure

1. Navigate to **All** > **Regulatory Change Management application** > **Compliance Workspace**.
   A new Compliance Management tab is displayed.
2. In the List view, navigate to **Lists** > **Taxonomy** page.
3. Navigate to one of the following modules:
   - **Regulatory Bodies**
   - **Content Types**
   - **Jurisdictions**
   - **Themes**
   - **Sectors**

   The name and parent body for the selected taxonomy category are displayed.
4. In the Name list, click a taxonomy element.
   Details of the selected taxonomy element are displayed on a separate page with the Details tab and Internal taxonomy related list.
5. To create a new internal taxonomy for the selected taxonomy class, click **New**.

**Create new internal taxonomy form**

| Field | Description |
|---|---|
| Name | Name of the internal taxonomy. |
| Taxonomy class | Taxonomy class populated by default for the selected category. |
| Parent | Parent record for which the new internal taxonomy is created. |

6. To save the taxonomy, click **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Regulatory Change Management classic user interface

The ServiceNow® Regulatory Change Management application enables you to check upcoming regulatory changes, assess their impact, and implement risk and compliance-related changes. The application ensures overall regulatory compliance.

Use the features and capabilities of the Regulatory Change Management application user interface such as setting up regulatory alerts, performing impact assessment, creating regulatory change tasks, creating action plan, managing action tasks, and closing of the regulatory change tasks to manage the regulatory changes across your organization.

## Regulatory alerts

Regulatory alerts are an aggregation of different regulatory events and documents that are sourced from multiple regulatory intelligence providers. Similar to web feeds, a regulatory alert is a record of these regulatory changes. Such changes are frequently updated, and the alerts help you stay informed about the regulatory landscape.

The Regulatory Change Management application transforms and maps the alerts. The application provides the information in regulatory alert tables.

The Regulatory Change Management life cycle starts with the regulatory alert record. Each regulatory alert record contains metadata that helps stakeholders to translate the changes, create an action plan, and implement actions to comply with the regulatory changes.

With the Regulatory Change Management application, you can use the regulatory alerts to inform the users about regulatory updates.

## Types of alerts and associated regulatory tasks

Different types of alerts are displayed under the Regulatory Alerts module in the Regulatory Change Management application.

You can use the following types of regulatory alerts:

- Regulatory event alerts: Signify alerts, provide updates to news, and provide insights on regulatory changes. Alerts are by default regulatory event alerts.
- Source document alerts: Signify changes to the citations. Citations are like various sections of an authority document. ServiceNow® GRC offers the Network Frontiers Unified Compliance Framework (UCF) integration. The integration creates authority documents after the import, and it creates corresponding citations under each authority document.

The main difference between a regulatory event alert versus a source document alert is about scope. Regulatory event alerts signify general alerts for general changes and for upcoming regulatory changes. In contrast, source document alerts signify changes that are specific to the citations. When an existing citation is updated or a new citation is inserted, it signifies a change in the source document.

The different types of alerts each involve a separate set of regulatory tasks. These tasks are created whenever a user with the sn_grc_reg_change.user role takes a alert and then marks it as applicable. These tasks are the following:

- Regulatory change task: This task is created for regulatory event alerts. The task is used to evaluate the changes and to update the GRC objects, such as policies, controls, and risk statements in the library.
- Source document import task: This task is created for source document alerts. The task is used to update an existing citation or to insert a new citation that is received from the provider into the regulatory library.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Alerts and user roles

Alerts can have different states. A main property of a alert is whether it is assigned or unassigned. For assigned alerts, the **Coordinator** field has a value. An alert can be assigned either to a manager with the sn_grc_reg_change.manager role or to a user with the sn_grc_reg_change.user role. In contrast, an unassigned alert is not assigned to anyone.

You can do various actions on unassigned alerts. These actions are the following:

- Update
- Applicable
- Defer
- Initiate Impact Assessment
- Not Applicable
- Cancel Regulatory Alert
- Delete

When an unassigned regulatory event alert is marked as applicable, a regulatory change task is created. When an unassigned source document alert is marked as applicable, a source document import task is created.

When an unassigned alert is marked as not applicable with due comments, its state is updated as Closed in the regulatory alert form.

Assigned alerts can have different states. These states are the following:

- New
- Deferred
- Impact Assessment
- In Progress
- Closed

In terms of user roles, all alerts can be accessed by users with either the sn_grc_reg_change.admin role or the sn_grc_reg_change.manager role. Users with the sn_grc_reg_change.user role can view assigned alerts that are assigned to them, but they cannot view unassigned alerts or alerts that are assigned to other people.

## Table cleaners for regulatory alerts

The alert records that are marked as not applicable must be cleaned at regular intervals. The Regulatory Change Management application provides table cleaners for cleaning the alert records automatically. Users specify the time and frequency for the cleanup activity.

Similarly, registry file records that have been processed can be cleaned at specified time intervals.

### Types of alerts, user roles, and states of regulatory alerts

Different users perform various actions on the alert records based on the type of the alert.

You can view the following types of alerts under the Regulatory Alerts module:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- All Assigned Alerts: Displays all assigned alerts in the instance where the **Coordinator** field is assigned to an appropriate user.
- Unassigned Alerts: Displays the unassigned alerts in the instance where the **Coordinator** field is empty. Mark the Overall impact as No impact, Low, Medium, High, or Critical.
- New Alerts: Displays new alerts in the instance where the **Coordinator** field is empty.
- Deferred Alerts: Displays the deferred alerts where the **Coordinator** field is assigned to an appropriate user, the state is Deferred, and a reminder date is listed to perform the action post deferral.
- Impact Assessment Alerts: Displays the alerts for regulatory events that are in Impact Assessment state.
- In Progress Alerts: Displays the alerts that are in In Progress state.
- Closed Alerts: Displays the alerts that are in Closed state.

The following table provides information on the user roles, the actions that these users can perform, and the description of these actions.

**User roles, actions, and description**

| User roles | Actions | Description |
|---|---|---|
| • sn_grc_reg_change.manager<br>• sn_grc_reg_change.user<br>• sn_grc_reg_change.admin | Update | Updates the details of the alert. |
| | Reassign | Reassigns the details of the alert. |
| | Defer | Defers a regulatory alert to a future date. |
| | Applicable | Marks the alert as applicable. |
| | Initiate Impact Assessment | Initiates an impact assessment on the alert. |
| | Not Applicable | Marks the alert as not applicable. |
| | Cancel | Cancels the alert. |

Managers can view all alerts. Users with the sn_grc_reg_change.user role can view assigned alerts that are assigned to them, but they cannot view unassigned alerts or alerts that are assigned to other people.

See the following table for information on the states of regulatory alerts.

**States of the alerts and their description**

| State | Description |
|---|---|
| New | Each incoming regulatory alert is by default assigned to a new state. Only the sn_grc_reg_change.admin or the sn_grc_reg_change.manager can assign an alert record. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**States of the alerts and their description (continued)**

| State | Description |
|---|---|
| Deferred | Some alerts do not require an immediate action and therefore, they are in the Deferred state and they are assigned to a later date. |
| Impact Assessment | The alert records that are of type regulatory event are assessed for applicability and are marked for an impact assessment. After an impact assessment, the alerts are marked as applicable or not applicable. |
| In Progress | Alerts with the In Progress state are being worked on. An sn_grc_reg_change.user is assigned to each alert. |
| Closed | Alerts that are not relevant to an organization are in the Closed state. Alerts that have associated tasks that have been completed are also in the Closed state. |
| Cancelled | Alerts that are in Cancelled state. |

**Note:** The attributes on the alert record are part of the metadata that is given by the third-party regulatory intelligence provider. These attributes help in determining the applicability of the alert to the organization. These records are non-editable in the Regulatory Change Management application.

### Perform actions on regulatory alerts

Perform various actions on unassigned and other types of regulatory alerts. For example, you can assign an unassigned alert, initiate impact assessment on an alert, and mark an alert as applicable, among other actions.

#### Before you begin

Role required: sn_grc_reg_change.manager or sn_grc_reg_change.user

#### About this task

A regulatory alert can be either a regulatory event alert or a source document alert. Some actions can be done on either type of alert, but some actions can only be done on regulatory event alerts. Users and managers can do many of the same actions, but there are some actions that can only be done by managers.

Managers can assign fields to the appropriate user. The appropriate user can then assess the applicability of the alert, initiate impact assessments, and complete the assigned regulatory tasks.

In the following procedure, steps 3 and after describe the various actions that you can take as a manager or user.

#### Procedure

1. Navigate to **All** > **Application** > **Regulatory Change Management** > **Regulatory Alerts**.
2. To assign an unassigned alert, click an alert in the Unassigned Alerts module. With the sn_grc_reg_change.manager role, you can set the **Coordinator** field to an appropriate user who has the sn_grc_reg_change.user role.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This action moves the alert to the All Assigned Alerts module.

3. To save and update the changes to the alert record, click **Update**.

| Field | Description |
|---|---|
| Click **Applicable** | Impact of the alert is applicable to your organization. If the alert is of a regulatory event type, then this action creates a regulatory change task. You can define and complete the regulatory actions that are associated with the change. If the alert is of a regulatory event type, then this action creates a regulatory change task. The state of the alert is updated to In Progress for both types of alerts. |

4. To defer an alert to a later date, do the following:
   a. Click **Defer**.
   b. Select a future reminder date and add a reason for the deferral.
   c. Click **Submit**.
   The alert is moved to the **Deferred** state in the application. Assigned users receive an email on the selected deferral date as a reminder to work on the alert. They can also cancel the alert.
5. To initiate an impact assessment on the alert, click **Initiate Impact Assessment**.
   This action is available only to managers and users of regulatory event alerts. This action is not available for source document alerts.
6. If the impact of the alert is not applicable to the organization, click **Not Applicable**.
   Specify a reason for marking the field as not applicable.
   The alert moves to the **Closed** state.
7. To cancel the alert, click **Cancel Regulatory Alert**.
   This action is available to managers and users of regulatory event alerts, and to managers of source document alerts; but it is not available to the users of source document alerts.
   This action moves the alert to the **Cancelled** state. The alert is moved to the Closed Alerts module.
8. To reassign an assigned alert to another user with the sn_grc_reg_change.user role, click **Reassign**.
9. To delete an alert, click **Delete**.

### Manage and assign regulatory event alerts

Assign regulatory event alerts that are received from the regulatory intelligence provider to an appropriate user. You can review other properties of the regulatory event alert.

## Before you begin

Role required: sn_grc_reg_change.manager

## About this task

Regulatory alerts are displayed under the Regulatory Alerts module in the Regulatory Change Management application.

As a manager, you can view and assign the regulatory event alerts to users with the sn_grc_reg_change.user role. The user can then perform actions on the regulatory event alerts.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **Application** > **Regulatory Change Management** > **Regulatory Alerts** > **Unassigned Alerts**.
   All the regulatory alerts in your instance are displayed. You can view the unassigned alerts and assign them to a specific user. An incoming alert is automatically assigned to the New state.
2. In the regulatory alert list, select a regulatory event alert by using the Type column.
   The alert record for the regulatory event alert is displayed.
3. To assign the alert, set the **Coordinator** field to the appropriate user.
   You can review the other properties of the alert to help you determine the appropriate user to assign to.

### Regulatory Alert form

| Fields | Description |
|---|---|
| Title | Title of the alert as received from the provider. |
| Description | Description and a brief summary of the event. |
| Provider URL | URL of the alert that is received from the provider. |
| Regulatory body URL | URL of the regulatory body that is associated with the alert. |
| Provider | Name of the alert provider. |
| Coordinator | User who is assigned the alert. |
| State | State of the alert. |
| Type | Type of regulatory alert. |
| Overall impact | Overall impact of the field. |
| Taxonomy | |
| Regulatory body | Organization that exercises a regulatory function, such as a government agency. |
| Sector | Different business segments for your organizations, such as banking and insurance. |
| Theme | Broad topics that you can use to classify your regulatory content. Possible themes are Privacy, Operational Resilience, and Regulatory Filings. |
| Jurisdiction | Location where a regulatory or legal body can extend the legal authority. |
| Content type | Different categories of content that a regulatory body can issue, such as legislative materials, regulations, and rules. |
| Dates | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Fields | Description |
|---|---|
| Source publication date | Date when the particular regulatory event is actually published by the regulatory body. |
| Effective date | Date when the particular regulatory event will be applicable. |
| Expiration date | Date when the particular regulatory event will expire. |
| Comments date | Date until when the comments can be provided for the regulatory event. |
| Compliance date | Date by which the regulatory event will be compliant. |
| Activity Journal | |
| Additional comments | Additional comments related to the alert. |
| Activities | Log of the activities related to the alert. |
| Related lists | |
| Regulatory Tasks | Related tasks for the alert. This field is available only when a alert is assigned to a coordinator and it is in In Progress state. |
| Related Documents | Details of the documents related to the alert, such as a citation, title, or type. |
| Impact Assessments | Impact assessment details that are associated with the regulatory event alert. |

4. Click **Update**.

### Result
The regulatory event alert is assigned to the selected user and it is listed under the **All Assigned Alerts** module in the application.

## Manage and assign source document alerts

Assign source document alerts that are received from the regulatory intelligence provider to an appropriate user. You can review other properties of the source document alert.

### Before you begin
Role required: sn_grc_reg_change.manager

### About this task
As a manager, you can view and assign the source document alerts to users with the sn_grc_reg_change.user role. The user can then perform actions on the source document alerts.

### Procedure
1. Navigate to **All** > **Application** > **Regulatory Change Management** > **Regulatory Alerts** > **Unassigned Alerts**.
   All the regulatory alerts in your instance are displayed. You can view the unassigned alerts and assign them to a specific user. An incoming alert is automatically assigned to the New state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. In the regulatory alert list, select a source document alert by using the Type column.
   The alert record for the source document alert is displayed.
3. To assign the alert, set the **Coordinator** field to the appropriate user.
   You can review the other properties of the alert to help you determine the appropriate user to assign to.

**Regulatory Alert form**

| Fields | Description |
|---|---|
| Title | Title of the source document type of alert as received from the provider. |
| Citation | Citation number for the source document that is received from the alert provider. |
| Provider URL | Provider URL for the alert. |
| Regulatory body URL | URL of the regulatory body that is associated with the alert. |
| Provider | Name of the alert provider. |
| Coordinator | User who is assigned the alert. |
| State | State of the alert. |
| Type | Type of the regulatory alert. For example, source document. |
| Taxonomy | |
| Regulatory body | Organization that exercises a regulatory function, such as a government agency. |
| Sector | Different business segments for your organizations, such as banking and insurance. |
| Theme | Broad topics that you can use to classify your regulatory content. Possible themes are Privacy, Operational Resilience, and Regulatory Filings. |
| Jurisdiction | Location where a regulatory or legal body can extend the legal authority. |
| Content type | Different categories of content that a regulatory body can issue, such as legislative materials, regulations, and rules. |
| Dates | |
| Source publication date | Date when the particular regulatory event is actually published by the regulatory body. |
| Effective date | Date when the particular regulatory event will be applicable. |
| Expiration date | Date when the particular regulatory event will expire. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Fields | Description |
|---|---|
| Comments date | Date until when the comments can be provided for the regulatory event. |
| Compliance date | Date by which the regulatory event will be compliant. |
| Activity Journal | |
| Additional comments | Additional comments related to the alert. |
| Activities | Log of the activities related to the alert. |

4. Click **Update**.

**Result**
The source document alert is assigned to the selected user and it is listed under the **All Assigned Alerts** module in the application.

## Impact assessments for the regulatory event alerts

A regulatory event alert may result in a regulatory change to an organization. You can evaluate the impact of the regulatory change on your business entities by performing an impact assessment.

The impact assessment process is used as a reporting tool for evaluating the impact of a proposed regulatory change. For a given regulatory event alert, the assigned user triggers an impact assessment to a subject matter expert who is an expert in a certain regulatory area. The expert then performs an impact assessment on the regulatory event alert.

If the regulatory event alert has an impact, the impact radius is calculated to find the associated control objectives that are related to the regulatory event. Based on the calculation, the application displays suggestions for what GRC objects will be impacted by the regulatory event.

When the impact assessment task is sent for approval, the impact assessment has the following typical sequence of events:

1. Assignment: The manager with the sn_grc_reg_change.manager role assigns a regulatory event alert to a user who has the sn_grc_reg_change.user role. The user views the assigned alert that is listed under the New Alerts module in the application.
2. Initiation of assessment: An event or a regulatory change that is described in the alert can cause an impact on the organization. The user can initiate an impact assessment to understand the impact of the change on the entities that are owned by different stakeholders. The user can mark the alert as applicable without initiating an impact assessment.
3. Assigning the assessment: The assessment task is automatically assigned to the owner of the entity, such as the owner of the business entity on which the assessment task is created. The alert is moved to the Impact Assessment state.

   **Note:** The entity owners who have the GRC Business User role can perform the impact assessment. For more information on the GRC Business User role, see .

4. Assessment creation: The entity owners gather details on the regulatory event, the proposed regulatory changes, and the severity of the impact. A regulatory event can impact one or more business entities. An assessment is created for each entity owner. For more information on configuring entity classes, see Configure an entity class.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Submitting the assessment: The entity owners assess the impact of the regulatory change and submit an impact assessment.
6. Decision making: Based on the assessment received from the entity owners, the manager or user decides the overall impact rating. The manager then marks the alert as applicable or not applicable.

Only entity owners can update the impact assessment task. The user can view the impact assessment task and its details only in read mode.

If an alert record has been sent for an impact assessment and you're waiting for a response, then the alert is in the Impact Assessment state.

**Note:** The Impact assessment action is applicable only to the regulatory event alerts.

### Assess the impact of a regulatory change

Assess the impact of a regulatory change and submit an impact assessment so that you can calculate the impact radius to find which control objectives are affected.

#### Before you begin

Role required: sn_grc.business_user

#### About this task

If the regulatory event alert has an impact, then the impact radius is calculated to find the associated control objectives that are related to the regulatory event. Based on the calculation, the application automatically displays suggestions for what GRC objects will be impacted by the regulatory event.

#### Procedure

1. Navigate to **All** > **Application** > **Regulatory Change Management** > **Regulatory Alerts**.
2. Select the regulatory alert that you want to assess.
3. Click **Initiate Impact Assessment**.
4. From the Entities list, select the entities that require an impact assessment.
5. Click **Create Assessments**.
   In the Impact Assessments related list in the regulatory alert record, the new impact assessment is listed.
6. Under the My Tasks module, log in as an assessor and click **Impact Assessment Tasks**.
   As an assessor, you can search for the impact assessment tasks in the application.
7. As an assessor, select the risk assessment task that is assigned under My Tasks, and then click **Assess**.
   The state of the risk assessment is updated to Inherent assessment. The **Inherent Assessment** tab is displayed. The following details of the risk assessment are displayed in the **Inherent Assessment** tab:
   - Regulatory Event Impact Context
   - Due date
   - Assessment summary
   - Inherent assessment
   - Activity journal
   - Results

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

In the Regulatory Event Impact Context record, you can click **Regulatory Alert** to view the regulatory alert associated with this impact assessment task.

8. Open the Inherent Assessment form and fill in the fields.

**Inherent Assessment form**

| Fields | Description |
|---|---|
| Factor | Factor for the impact. A factor describes the type of the risk posed for the business. Choices are as follows:<br>◦ **Legal impact**<br>◦ **Reputational impact**<br>◦ **Financial impact**<br>◦ **Business impact** |
| Response | Response for the impact. Choices are as follows:<br>◦ **Low**<br>◦ **Medium**<br>◦ **High**<br>◦ **Critical** |
| Qualitative Weight | Qualitative weight for each factor. For example, 25% for each factor. |
| Qualitative Score | Qualitative score for each factor. |
| Quantitative Score | Quantitative score for each factor. |
| Comments | Comments and additional information for the impact. Click **Add Comments** to enter comments for each factor. |
| Results | |
| Computed inherent risk | The computed inherent risk for the risk assessment task. |
| Comments | Additional comments related to the assessment. |

**Note:** For risk assessment, the Advanced Risk Assessment engine is used. Administrators can update the Risk Assessment Methodology (RAM) and update the Inherent Assessment factors manually.

9. To save the assessment, click **Save and calculate**.
   This action calculates the risk and displays the computed inherent risk under the **Results** tab. This action saves the calculation, but it does not submit the assessment.
10. Click **Mark as complete**.
    This action saves the form. The calculated inherent risk is displayed under the **Assessment Summary** tab.
11. As a user, click **Applicable** to mark the impact assessment task as applicable.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Result**
A regulatory change task is created for the alert. The task is displayed in the Regulatory Tasks related list of the alert.

### Impact radius calculation and approval

Calculate the impact of regulatory changes and recommend related tasks using impact radius calculation. An impact radius is calculated for both types of regulatory tasks, which are regulatory change tasks and source document import tasks.

The Regulatory Change Management application supports the impact radius calculation process. Calculating the impact radius is a method of recommending action tasks to the users.

The regulatory events that could have an impact on the compliance or risk posture of your organization should be assessed. Calculating the impact radius is a method for assessing the impact of the regulatory event on the GRC objects and for suggesting action tasks based on the assessment of the impact.

The following steps are used for the process of impact radius calculation and for automatic task recommendation:

1. The existing regulatory library is searched for the matching citation names, the name of the provider, and the source field.

   For a regulatory event alert, the citations associated with the alert are listed in the Related Documents list. For a source document alert, the citations associated with the alert are displayed in the **Citation** field.

2. If the matching citation is from the same provider or if the provider source field is empty, then new action tasks are recommended to the user.
3. The action tasks that are recommended by the application are automatically created with the control objective as the action target. The tasks are displayed in the action tasks related list.

   The applicability of the created action tasks is set to **False** by default.

4. The user with the sn_grc_reg_change.user role reviews the actions tasks. If the tasks are applicable, then the user sets the **Applicable** field to **True** and requests an approval on the parent regulatory task.
5. The approver can approve the parent regulatory task, reject it, or ask for more information on the task.

   After the parent regulatory task is approved, its applicable child action tasks are moved to the Ready state. For non-applicable child action tasks, those tasks get canceled.

6. When an action task is completed, the associated regulatory tasks get closed.

Business users and managers with the sn_grc_reg_change.manager role can review the action tasks. They can manually add action tasks in case the application does not display suggestions for any action tasks. Both the approver and the compliance user can read the comments for each object to get more information about the associated action tasks.

## Regulatory change tasks

When a manager or user marks an unassigned alert as applicable, a regulatory change task is created. A regulatory change task is used by the stakeholders to analyze and identify the

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

changes that should be performed on the alerts. The stakeholders can then create action tasks.

A regulatory change task serves as the parent for all the action tasks that have been created to complete the identified changes. For example, an action task can involve making updates to the policies, controls, and risk statements in the regulatory library.

A manager with the sn_grc_reg_change.manager role assigns a regulatory change task to an identified user with the sn_grc_reg_change.user role in the system. The regulatory change task displays the details of the task such as the assignment group, the approver, the assignee, and other relevant information.

After a regulatory change task is completed, the associated regulatory alert can be closed.

#### Users and associated actions for the regulatory change tasks

Managers with the sn_grc_reg_change.manager role and the users with the sn_grc_reg_change.user role can view and perform certain tasks in the Regulatory Change Tasks module.

## Views and actions available to managers

Managers with the sn_grc_reg_change.manager role can view the following tasks in the Regulatory Change Tasks module:

- All Assigned Tasks
- Unassigned Tasks
- New Tasks
- Respond Tasks
- Pending Approval Tasks
- Implementation Tasks
- Closed Tasks
- My Approvals

Managers can perform the following actions on a regulatory change task:

- Assign the regulatory change task to a user with the sn_grc_reg_change.user role.
- Add instructions for the assignee on the task.
- Get added to the watchlist.
- Add work notes.
- Add a future due date to complete the work on the regulatory change task.
- Add an approver, typically another manager, to approve the regulatory change task.
- Update the work notes.

## Views and actions available to other users

Users with the sn_grc_reg_change.user role can view the following tasks in the Regulatory Change Tasks module:

- New Tasks
- Respond Tasks
- Pending Approval Tasks

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Implementation Tasks
- Closed Tasks

If the user is assigned the regulatory change task, then the user can log in and perform the following actions on the regulatory change task:

- View the regulatory change task under New tasks.
- Update the work notes.
- Click **Respond** to move the task to the Respond state.
- Verify if an action task should be created for the regulatory change task.
- Evaluate if the incoming alert has an impact on the GRC library of the current system.
- View the details of the impact assessment performed by entity owners.
- Create necessary action tasks that are related to the Compliance and Risk areas in the GRC library, and then assign them to an appropriate group.

### Manage the regulatory change tasks

Manage the regulatory action tasks in the Regulatory Change Tasks module so that you can use these tasks to identify and comply with the regulatory changes.

#### Before you begin

Role required: sn_grc_reg_change.manager or sn_grc_reg_change.user

#### About this task

Regulatory change tasks are automatically created whenever a regulatory event alert is marked as applicable after the applicability assessment. Regulatory Compliance team members craft an action plan to identify the changes that need to be implemented so that your organization complies with the regulatory change.

#### Procedure

1. Navigate to **All** > **Application** > **Regulatory Change Management** > **Regulatory Change Tasks**.
2. Select a regulatory change task.
3. On the form, fill in the fields.

**Regulatory Change Task form**

| Field | Description |
|---|---|
| Assignment group | Assignment group of the task. The group is selected from the Group Hierarchy table. |
| Approver type | User or group who approves the task. |
| Due date | Due date for the regulatory change task. |
| Regulatory alert | Name of the regulatory alert. |
| Instructions | Instructions for the task. |
| Assigned to | Name of the user who is assigned the task. |
| Approver | Approver of the regulatory change task. When the approver type is Group, the request is sent to the group members. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Approved on | Date when the regulatory change task is approved. |
| Watch list | Watch list to add interested users. |
| Worknotes list | Users interested in the work notes. |
| Work notes | Log of the work notes. |
| Activities | Log of the activities. |
| Related list | |
| Action Tasks | Action tasks related to the regulatory change tasks. Click **New** to create an action task in response to the regulatory change task.<br>**Note:**<br>If there are action tasks that are in progress when the parent regulatory task is closed manually, all the associated action tasks are moved to the Cancelled state with the following warning message: `Action tasks for this Regulatory Change Task/ Document Import Task are in-progress. Clicking OK will cancel them. Do you want to proceed?`<br>If there are no action tasks associated or if the action tasks are closed, the following message is displayed: Are you sure you want to close this task? Click OK to close the task. |
| Issues | Issues observed during the regulatory change workflow or source document workflow. |
| Approvers | Approval records that get created when an approval is requested. |

4. Click **Update**.
5. If you want to add new action tasks that are related to the regulatory change task, click **New** in the Action Tasks related list.
6. To request an approval on the regulatory change task, log in as an approver and click **Request Approval** to request an approval.
   The state of the regulatory change task is updated to the Awaiting Approval state. In the Approvers related list of the regulatory change task, the state of the approval is updated to Requested. The manager with the sn_grc_reg_change.manager role, the user with the sn_grc_reg_change.user role, or the admin user with the sn_grc_reg_change.admin role can view the request under **Regulatory Change Tasks** > **My Approvals**.
7. Click **Approve** to approve the request.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Result**
The request is approved. The regulatory change task moves to the Implementation state. When the action task associated with the regulatory change task is completed, the regulatory change task is closed.

## Source document import tasks

The Regulatory Change Management application processes the alerts that are externally sourced. Source document import tasks are automatically created whenever a source document alert record is marked as applicable. The source document can refer to the legislative and regulatory materials.

When a source document type of regulatory alert is received, it provides the citation title and the number of the citation. The citation can already be available in the GRC library or it can be a newly created citation. Each alert record contains metadata about the source document that helps the key stakeholders to import the record into the regulatory library. The metadata includes the citation name and other information.

Source document alerts are used to create source document import tasks. A source document import task is used to ingest a particular source document that is received from the provider into the regulatory library. This task is performed by the Compliance team members. They import a source document into the regulatory library in ServiceNow as a citation object.

A source document import task is created from a regulatory alert record. The task goes through the source document import workflow or life cycle.

1. All the unassigned alert records that are of source document type are assessed for applicability.
2. If a source document alert record is marked as applicable, a source document import task is automatically created.

The source document import life cycle starts from the regulatory alert record. When the manager with the sn_grc_reg_change.manager role marks an unassigned source document alert as applicable, a source document import task gets created.

Users can view the import document task in the Ready to Import state, evaluate the citation associated with the alert, and decide the future course of action for the import document task.

### Users, associated actions, and states for the source document import tasks

Managers with the sn_grc_reg_change.manager role and the users with the sn_grc_reg_change.user role can view and perform certain actions on the source document import tasks.

## Views and actions available to managers

Managers with the sn_grc_reg_change.manager role can view and sort the following types of source document import tasks:

- All tasks
- Unassigned tasks
- All assigned tasks
- Ready to Import tasks
- In-progress tasks

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Implementation tasks
- Pending approval tasks
- Closed tasks
- My approvals

Managers can view the import document task under the My Approvals module.

Managers can perform the following actions on the source document alert:

- Assign the alert to a user.
- Update the alert with additional details.
- Reassign the alert to another user.
- Defer the alert to a later date by adding a reason and the comments.
- Mark the alert as applicable or not applicable after performing an initial assessment. This action changes the state of the alert to In Progress.

## Views and actions available to other users

Users with the sn_grc_reg_change.user role can view the import document task under the Implementation Tasks.

Users can view the new source document alert under the New Alerts module.

**Note:** For source document type of alerts, an impact assessment is not needed.

Users can perform the following actions on a new alert:

- Update the details of the alert.
- Mark the alert as applicable.
- Mark the alert as not applicable.

## States of the source document import task

The states of the source document import task are the following:

- Ready to Import
- In Progress
- Awaiting Approval
- Implementation
- Deferred
- Closed

If the alert is marked as applicable, and if the source document task created as part of the process moves to the Closed state, then the regulatory alert record is automatically moved to the Closed state.

### Manage the source document import tasks

Manage the source document tasks, the associated source document alerts, and other relevant details in the Regulatory Change Tasks module. Use these tasks to identify and comply with the source document changes.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_grc_reg_change.manager or sn_grc_reg_change.user

### About this task
A source document import task is used to ingest a particular source document that is received from the provider into the regulatory library.

### Procedure
1. Navigate to **All** > **Application** > **Regulatory Change Management** > **Source Document Import Tasks**.
2. Select a source document import task.
3. On the form, fill in the fields.

**Source Document Import Task form**

| Field | Description |
|---|---|
| Assignment group | Assignment group for the record. The group is selected from the Group Hierarchy table. |
| Approver type | Approver type for the task. Choices are as follows:<br>◦ **User**<br>◦ **Group** |
| Due date | Due date for the source document import task. |
| Regulatory alert | Name of the regulatory alert. |
| Instructions | Instructions for the task. |
| Assigned to | Name of the person who is assigned the task. |
| Approver | Approver of the source document import task. When the **Approver type** field is set to **Group**, the request is sent to the group members. |
| Approved on | Date when the source document import task is approved. |
| Activity Journal | Activity log where the sn_grc_reg_change.user can add comments. |
| Related list | |
| Similar source documents | Records of similar source documents. |
| Action Tasks | Action tasks related to the import document tasks. Click **New** to add new action tasks. |
| Issues | Issues observed during the regulatory change workflow or the source document workflow. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Approvers | Approvers of the import document task. This list displays the approval records that get created when an approval is requested. |

4. To apply your changes, do one of the following:
   - To update the selected source document import task, click **Update**.
   - To save the changes, click **Work in Progress**.
5. To request an approval for the source document import task, click **Request Approval**.

**Result**
A new citation is inserted or an existing citation is updated.

## Action tasks in Regulatory Change Management

The Compliance and Risk teams assign and perform the action tasks. These tasks are used to track and complete the changes that are identified in the action plan.

Action tasks are related to regulatory change tasks and to source document import tasks. Users with the sn_grc_reg_change.manager or sn_grc_reg_change.user role create action tasks in response to regulatory change tasks and to source document import tasks. These tasks are related to the Compliance and Risk areas in the GRC library. The Compliance Manager and Risk Manager assign the tasks to the correct Risk or Compliance group.

There are two categories of action tasks in the Regulatory Change Management application:

- Compliance: Contains all compliance-related action tasks. Compliance users can select a specific Compliance object in the GRC library, such as policies and controls.
- Risk: Contains all risk-related action tasks. Risk users can select a specific Risk object in the GRC library, such as risk statements.

Auto-creation of action tasks was enabled only for control objectives with the GRC: Regulatory Change Management, Version 11.0.3 release. Starting with the GRC: Regulatory Change Management, Version 12.0.2 release, action tasks are created automatically also for potentially impacted risk statements and policies.

Managers with the sn_grc_reg_change.manager role can view and sort the action tasks using the following tabs:

- **All assigned tasks**
- **Unassigned compliance tasks**
- **Unassigned risk tasks**
- **Ready tasks**
- **In Progress tasks**
- **Closed tasks**

### Create an action task

Create an action task that is related to the regulatory change tasks and source document import tasks so that you can complete the regulatory tasks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_grc_reg_change.manager or sn_grc_reg_change.user

### About this task
The regulatory action tasks are created as a follow-up to complete the changes that have been identified as part of the impact assessment for regulatory change tasks. Once these specific changes are identified, you can create and manage these action tasks as a manager or user.

### Procedure
1. Navigate to **Application** > **Regulatory Change Management** > **Action Tasks**.
2. Select an action task.
3. On the form, fill in the fields.

**Action Tasks form**

| Field | Description |
|---|---|
| Regulatory Task | Number of the regulatory task. |
| Category | Category type of the action task, such as compliance or risk. |
| Assignment Group | Group that is assigned the action task. |
| Priority | Priority of the action task. |
| Due date | Due date of the action task. |
| Compliance action target | Specific GRC object to be selected. For example, Authority Document, Citation from the list menu, and the associated document. |
| Assigned to | User who is assigned the task. |
| Short description | Short description of the action task. |
| Instructions | Instructions for the action task. |
| Activity Journal | |
| Watch list | List of users who receive notifications about the updates. |
| Work notes | Log of the work notes. |
| Worknotes list | Users who receive notifications about the work notes. |

You can update the following fields:

- **Category**
- **Action target**
- **Short description**
- **Instructions**
- **Work notes**

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **Worknotes list**
- **Watch list**

4. Click **Save**.
   The action task is saved and it is displayed under the Action Tasks tab in the Regulatory Change Tasks page.

## Map the taxonomy

Create an internal taxonomy when you are setting up the Regulatory Change Management application. Map the external taxonomy to the internal taxonomy so that the Regulatory Change Management application refers to only one taxonomy.

### Before you begin

Role required: sn_grc_reg_change.admin

### About this task

The Regulatory Change Management application stores the taxonomy and it provides a way to map the taxonomies using the UI component.

### Procedure

1. Navigate to **Application** > **Regulatory Change Management** > **Taxonomy** > **Taxonomy Classes**.
   The taxonomy classes available that are shipped out-of-the-box are displayed:
   - Regulatory Bodies
   - Content Types
   - Jurisdictions
   - Themes
   - Sectors
2. Navigate to the following taxonomy tables if you want to view or update the taxonomy class name:
   - **Regulatory Bodies**
   - **Content Types**
   - **Jurisdictions**
   - **Themes**
   - **Sectors**

   As an example, when you click Jurisdiction, the Class name field displays Jurisdiction as the taxonomy class.

   **Note:** Only users with the sn_grc_reg_change.admin roles can update the taxonomy tables.

3. Click **Update** to update the class name.
4. Click **New** under Taxonomy class related list.
   A new Taxonomy class record is displayed on a separate page.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Taxonomy class record**

| Field | Description |
|---|---|
| Name | Name of the taxonomy class. |

The new taxonomy class is displayed on the Taxonomy Class page.

5. Open the Taxonomy Class page to create a new Taxonomy class mapping record.
6. On the form, fill in the fields.
   Depending on what regulatory table was previously selected, the form title is different.

**Taxonomy class mapping record**

| Field | Description |
|---|---|
| Provider | Provider of the alerts. |
| External taxonomy class | External taxonomy class that is mapped with the internal taxonomy class. |
| Taxonomy class | Taxonomy class provided that is out-of-the-box such as Jurisdictions or Content type. |

7. Click **Submit** to map the external taxonomy class to the internal taxonomy class.
   The external taxonomy class is mapped to the internal taxonomy class.

## Create an issue related to the regulatory tasks

Create an issue as part of the regulatory change tasks and source document tasks workflow to capture any problems or exceptions that are observed during the workflow. You can create and view issues related to regulatory tasks using the issues related list.

### Before you begin

Role required: sn_grc_reg_change.manager, sn_grc_reg_change.user

### About this task

A new module titled as Issue is introduced in the Regulatory Change Management application.

### Procedure

1. Navigate to **Application** > **Regulatory Change Management** > **Issue** to create and view issues related to the regulatory tasks using the issues related list.
2. Use the following modules to get a filtered list of the issues.

**Create and view issues related to Regulatory Tasks**

| Field | Description |
|---|---|
| My Open Issues | View open issues assigned to a user. |
| All Open Issues | View all open issues assigned to a user. |
| All Unassigned Issues | View all unassigned issues assigned to a user. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| All Grouped Issues | View all grouped issues assigned to a user. |
| All Issues | View all issues related to the Regulatory Tasks. |

**Result**
You can view the issues related to the Regulatory tasks in the respective modules.

## Administration module

Use the Administration module to manage third-party providers and the configuration of entity classes.

Regulatory Intelligence providers deliver regulatory alerts that include a variety of regulatory changes. Each regulatory alert record contains the taxonomy section for the regulatory taxonomy associated with the alert. This taxonomy helps in classifying and categorizing the alert. The internal taxonomy design contains the following five elements:

- Regulatory Body
- Sector
- Theme
- Content Type
- Jurisdiction

When setting up the Regulatory Change Management application, you have to map the external taxonomy to your own internal taxonomy for standardization. The design elements are created and mapped from the provider's external taxonomy during the setup process.

After you set up the internal taxonomy, the next step is to update the provider configuration record with the name and description of the providers. To maintain a generic provider configuration, a provider record is used. Providers can send the data via multiple combinations, such as via a single file or as an API. To learn more, see Map the taxonomy.

You can use the Administration module to configure various records. You can do the following:

- Update provider configuration record to define and receive the data from the providers.
- Configure the entity classes that may be impacted due to the regulatory changes.

### Configure a provider taxonomy configuration record

Configure a provider taxonomy configuration record to define and map the external taxonomy to an internal taxonomy class.

**Before you begin**
Role required: sn_grc_reg_change.admin

**Procedure**

1. Navigate to **Application** > **Regulatory Change Management** > **Administration** > **Provider Taxonomy Configuration**.
2. Click **New** on the page.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Provider taxonomy configuration record form**

| Field | Description |
|---|---|
| Provider | Provider of the taxonomy configuration record. |
| Default taxonomy configuration | Check box option to use the default taxonomy configuration. Clear the default taxonomy configuration option to see the Taxonomy Loader configuration. |
| Taxonomy | Internal taxonomy to which the external taxonomy is mapped. Unlock the list to add the taxonomy. |
| Taxonomy Loader | Taxonomy Loader configuration field when the default taxonomy configuration option is unchecked. Select the import mode for importing the taxonomy data:<br>◦ Data source: Use Data source if the taxonomy can be imported via ServiceNow platform data source.<br>◦ Custom script: Use Custom script if the taxonomy import needs custom logic.<br>For Data source: Update the following fields:<br>◦ Data source: Data source to be defined such as Azure AD, Auth0.<br>◦ Scheduled data import: The import job that runs the data source frequently.<br>For Custom script: Update the following fields:<br>◦ Taxonomy file required: Select the check box if the data to be imported via the selected mode needs a file to be attached.<br>◦ Variables: Use the variables defined in the script.<br>◦ Script: Script to be populated. This is a required step. |

4. Click **Submit**.

**Result**
The new provider taxonomy configuration record is listed on the Provider taxonomy configuration page.

### Configure an entity class

Configure entity classes on which impact assessments are performed. You can add the classes of the entities that must be selected in impact assessments.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_grc_reg_change.admin

### About this task
As an administrator, you can set up the entity classes when setting up the configuration. Business entities are evaluated by impact assessments. You must configure these entity classes before the entity owners can perform their impact assessments or risk assessments. These entity classes are shipped by the GRC application by default. Based on the customer configuration, more entity classes are added to the application. If a user creates more classes, they are also displayed in the list.

### Procedure
1. Navigate to **All** > **Application** > **Regulatory Change Management** > **Administration** > **Entity Class Configuration**.
2. In the Available column, select one or more entity classes.
3. Move the selected entity classes to the Selected column.
   The selected entity classes are displayed in the Selected column.
4. Click **OK**.

### What to do next
After the entity classes are configured, the entity owners can evaluate the impact of the proposed regulatory changes on the entities that they own. They can then perform a risk assessment. Based on the assessment received from the entity owners, the manager or the user decides the overall impact and marks the alert as applicable or non-applicable.

## Set up the RSS feeds

Set up the RSS feeds data in the Regulatory Change Management application installed in your instance. Install the RSS feeds plugin for activating RSS feeds data in the Regulatory Change Management application.

### Before you begin
Prerequisite for activating the GRC: Regulatory Change Management integration with RSS Feeds  plugin: The Regulatory Change Management application should be installed first in your instance.

Role required: sn_grc_reg_change.it_admin, sn_grc_reg_change.manager, sn_grc_reg_change.user

### About this task
RSS (RDF Site Summary or Really Simple Syndication) feeds are Web feeds that allow users and applications to access updates to websites in a standardized and computer-readable format. Websites use RSS feeds to publish frequently updated information, such as blog entries, news headlines, and episodes of audio and video series.

### Procedure
1. Navigate to **Application** > **Regulatory Change Management** > **RSS Feeds** to fetch RSS feeds data in the Regulatory Change Management application.
2. Download and install the GRC: Regulatory Change Management integration with RSS Feeds  plugin from the store.
   Once the GRC: Regulatory Change Management integration with RSS Feeds  plugin is installed, the RSS Feeds module is displayed under the Regulatory Change Management application module in the UI. The following submodules are displayed under RSS Feeds.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Submodules under RSS Feeds**

| Field | Description |
|---|---|
| Feed Setup | Module to set up the flow to pull the RSS feeds. |
| Connection & Credential Aliases | Alias to configure the URL from where you get the specific RSS data. |
| Provider Taxonomy Configuration | Module to set up the provider taxonomy configuration. |
| Feed Sources | New feed source record. |
| Feed Request Response | Module that contains the responses from the RSS feeds sources. |

3. From the Feed Setup module, complete the following steps.
   a. Select the **RCM RSS Flow** in the Flow Designer UI page.
   b. Click **Done** and click **Activate** to activate the flow.
   The RCM IT Admin schedules the RCM RSS Flow to run on a daily, weekly, or monthly basis and sets up the time for the flow.
4. Click the **Connection & Credential Aliases** module and click **Create New Connection & Credential** under Related Links.
5. Enter the connection information in the Create Connection and Credential record form as outlined in the table and click **Create**.

**Connection & Credential Aliases module**

| Field | Description |
|---|---|
| Name | Connection name in the text format, for example, Federal Reserve, FDA (Food and Drug Administration). |
| Connection URL | Connection URL from where the feeds are fetched, for example, https://www.rbi.org.in/pressreleases_rss.xml |

A new connection is created and listed under the Connection & Credential Aliases related list.

6. Enter information in the Provider Taxonomy Configuration to set up the provider taxonomy configuration.
   See Configure a provider taxonomy configuration record for more information.
7. Enter information in the Feed Sources new record form as outlined in the table.

**Feed Sources new record**

| Field | Description |
|---|---|
| Name | Name in the text format for the new record. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Connection | Connection that you have newly created under the Connection & Credential Aliases module. Enter the provider URL of the feed.<br>**Note:** Only public URLs are supported at this point. |
| Active | Check box to mark the feed source as active |
| Provider | New provider record.<br>◦ Name<br>◦ Description<br>◦ Taxonomy source: Single, Multiple, or Default. Select Default option to map the taxonomy and select the design elements of the taxonomy, such as, Jurisdiction, Regulatory Body, Sector, Theme, and Content Type.<br>Click Submit to add the new provider. |

**a.** Click **Submit** in the Feed Source record form to create a new feed source record.

8. In the Feed Request Response module, view the response from the RSS feeds sources or click **New** to create a new feed request response.

**a.** On the form, fill in the fields.

**Feed Request Response form**

| Field | Description |
|---|---|
| RSS Feed Source | RSS feed source for receiving the feeds. |
| Response | Response to the RSS feeds. |

**b.** Click **Submit**.
A new Feed Request Response record is created.

**Result**
Once the feed source is set up and the RCM RSS Flow gets executed at a scheduled time, the RSS feeds data is received in the Feed Request Response table. The RSS feeds data parsed from the Feed Request Response table is displayed in the Regulatory Feeds table.

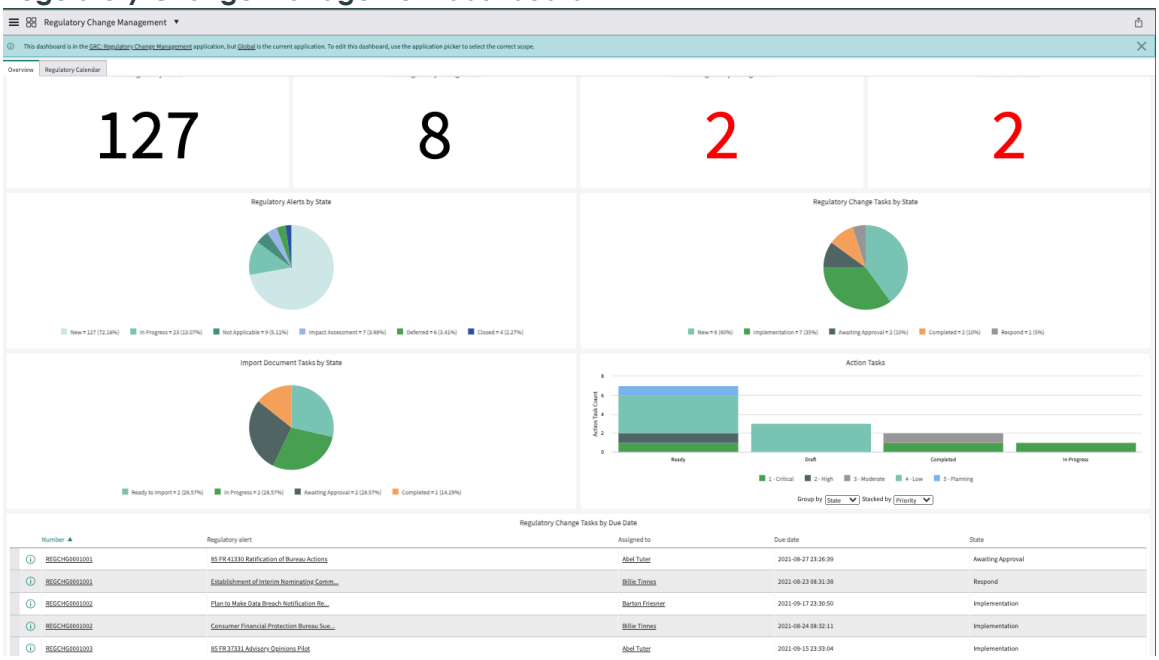
## Regulatory Change Management dashboard

The Regulatory Change Management dashboard provides the current view of the regulatory landscape.

To view the Regulatory Change Management dashboard, navigate to **Regulatory Change Management** > **Overview**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Regulatory Change Management dashboard




## Overview of regulatory changes

For examples of how different people in your organization would use this dashboard, see these use cases.

### Dashboard use cases

| User | Dashboard use |
|---|---|
| sn_grc_reg_change.manager | The RCM Manager can view the new regulatory Alerts and understand the state of the alerts and the different regulatory tasks. It also provides a calendar view of the regulatory tasks with their due dates. |

The Overview page provides a summary of the regulatory events and tasks, such as the following:

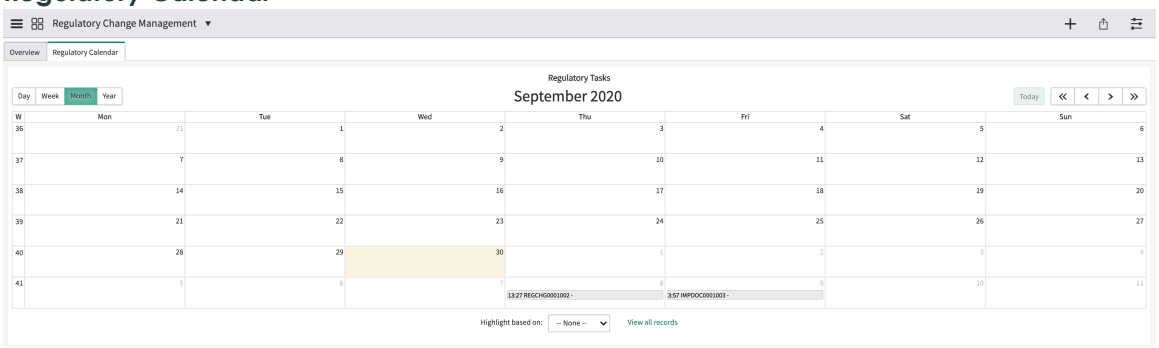
- New Regulatory Alerts
- New Regulatory Change Tasks
- Overdue Regulatory Change Tasks
- Critical Action Tasks
- Regulatory Alert by State: Displays the alerts that are grouped by state, number, and percentage
- Regulatory Change Tasks by State: Displays the tasks that are grouped by state, number, and percentage
- Import Document Tasks by State: Displays the tasks that are grouped by state, number, and percentage
- Action Tasks: Groups and stacks the action tasks by the State and Priority fields
- Regulatory Change Tasks by Due Date: Displays a report of the regulatory change tasks

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Regulatory Calendar

The Regulatory Calendar provides an overview of the regulatory tasks. The calendar helps you with planning and managing these tasks.

**Regulatory Calendar**




Use the options in the top left of the calendar to display the calendar in a daily, weekly, or monthly view. Click a specific task to view its details.

You can filter and highlight the regulatory tasks based on the following details:

- Approval
- Escalation
- None
- Priority
- Work notes

Click **View all records** to view all the regulatory tasks in a list format displayed in a separate tab.

# Risk Management

Use the Governance, Risk, and Compliance: Risk Management application to continuously monitor to identify high-impact risks, improve your risk-based decision-making, and reduce reaction time effectively. The application also provides structured workflows for the management of risk assessments, risk indicators, and risk issues.

### Risk Workspace

Starting with version 13.0.5, the Risk Workspace has been added for Risk Management users. The Risk Workspace offers a simplified user experience for you to perform your daily tasks and activities. For more information on the new workspace, see GRC Risk Workspace.

### Benefits of Risk Management

The benefits of Risk Management are:

- Faster risk-based decision-making: Prioritize activities based on automated risk scores to work on the most critical risks first.
- Increased performance: Risk management embedded in automated cross-functional activities eliminates work interruption.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Effectively communicate risk: Real-time insights and role-based dashboards make reporting at all levels easier and faster.
- Stay on top of risks: Mobile interfaces provide the information you need to do your job anytime and anywhere.

| | | |
|---|---|---|
| Explore<br>  <br>Learn about how risk managers, risk users, and risk administrators use the Risk Management application. | Configuring Risk Management<br>  <br>Configure your Risk Management application. | Integrate Risk Management<br>  <br>Extend Risk Management capabilities by integrating with other applications. |
| Using Risk Management<br>  <br>Work on risk assessments, risk events, and so on. | Analytics and reporting solutions for Risk Management<br>  <br>Highlight the critical risks with dashboards and reports. | Risk Management reference<br>  <br>Get details about components like fields, tables, and properties. |

## Implement Risk Management

Use the Risk Management implementation to quickly implement the GRC Risk Management and Advanced Risk applications.

## Additional resources

- Ask or answer questions in the GRC community
- Search the Known Error Portal for known error articles
- Contact Customer Service and Support
- Developer training
- Developer documentation

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Exploring Risk Management

The Risk Management product provides a centralized process to identify, assess, respond to, and continuously monitor Enterprise and IT risks that may negatively impact business operations. The application also provides structured workflows for the management of risk assessments, risk indicators, and risk issues.

## Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

## Who uses Risk Management

The complete risk process involves all areas of your organization working together.

- Audit committee
- IT steering committee
- Risk officers (conduct risk assessment and identify all that can go wrong in business)
- All levels of management (assist the risk officers with the identification of what can go wrong in their processes)

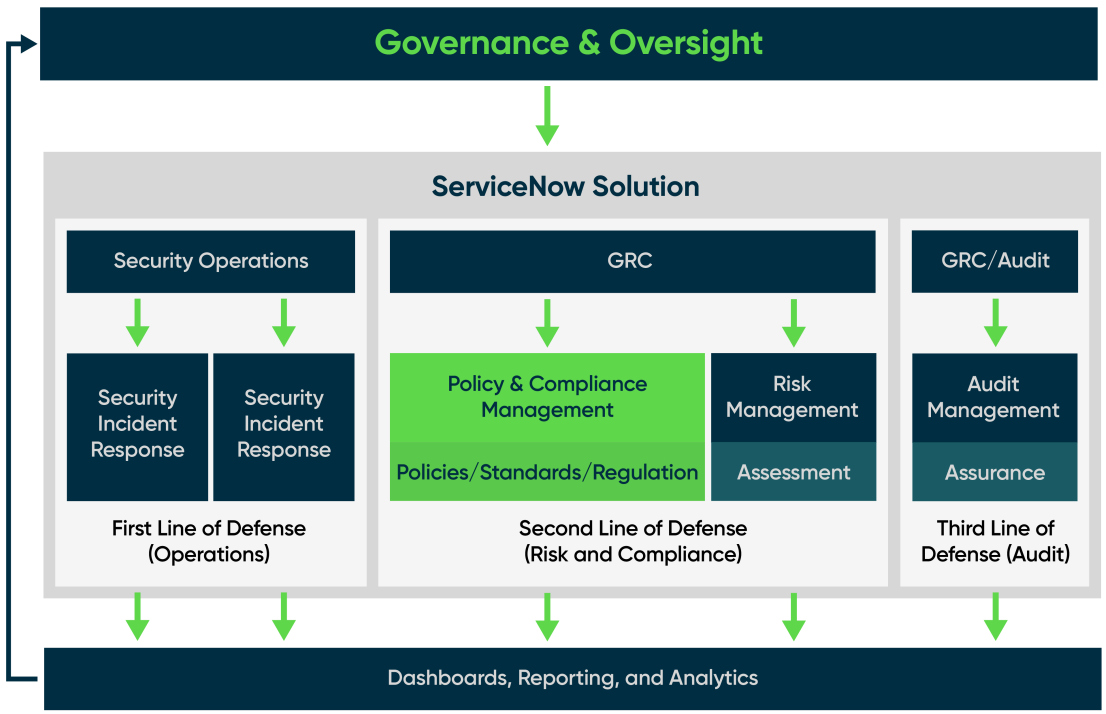
## Key activities for Risk Management

Once the key roles are identified, work to identify the following items:

- Determine what level of risk the organization is willing to accept? Get risk data in place and then determine what is acceptable.
- Develop a risk management policy, through risk frameworks and risk statements.
- Develop risk assessment and response procedures.
- Implement controls to reduce your organization's exposure to risk. Repeat on a regular interval.
- Measure your risk exposure and improvements.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Risk Management and the Now Platform




The Risk Management and the Advanced Risk applications enable you to do the following.

- Manage risks, risk statements, and risk frameworks: The risk library contains all risk frameworks and risk statements. Risk frameworks are used to group risk statements into manageable categories, while risk statements group the individual risks. The risk register is the central repository for all potential risks that could occur at any time, anywhere in the organization.
- Manage risk events: Risk events are potential or actual financial and non-financial losses, near-misses, and gains that occur within an organization.
- Risk hierarchy and scoring: Starting with New York, risk managers can create hierarchies that include different types of risk (operational risk, IT risk, or strategic risk). Once the underlying risks are assessed, the risk scores are automatically rolled up across the risk statement hierarchy, providing better tactical and strategic decision-making.
- Manage classic risk assessments: Risk assessments are surveys that gather evidence to determine risk. The Risk Assessment Designer provides a single interface that users can use to create, and edit attestations, as well as change scoring parameters. The question bank offers a library of questions for various categories, so you do not have to build each questionnaire from scratch. Risks start in a **Draft** state then move to **Assess**, which sends a notification to the Assessment respondents.
- Manage Advanced Risk Assessments: With Advanced Risk Assessment, create an integrated risk platform. This integrated platform supports various kinds of risk assessment methodologies and enables you to integrate risk assessment as a part of your overall decision-making process.
- Manage policy exceptions and extensions: Policy exceptions and extensions provide temporary relief for a non-compliant control. The policy exception captures the rationale, comments, and evidence to support the acceptance or rejection of a policy exception request. Also, extension to an approved policy exception can be requested before the policy exception validity period. The control owner, the compliance manager, and the risk manager may be involved in the policy exception and extension workflow.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Use entity and risk dependencies using the GRC: Workbench: The GRC: Workbench utilizes CMDB information to show the upstream and downstream relationships across all applications. These relationships enable consistent risk mapping and modeling across the enterprise.
- Risk indicators, control indicators, and indicator templates: Continuous monitoring involves activities related to identifying and creating key risk and control indicators. Supporting information can be collected for those indicators through automatic data collection or manual tasks. Indicator results are then used to create issues for controls, update risk scores, and provide supporting information for audit activities and control testings.
- Manage risk issues and remediation: Issues can be created manually to document audit observations, remediations, or to accept any problems. They are automatically generated from indicator results, attestation results, or control test effectiveness.
- Manage continuous monitoring for risks between Risk Management and Vulnerability Response: Continuous monitoring for risks is a feature integration between the GRC: Risk Management and the Security Operations Vulnerability Response products, which uses indicators to quickly identify high impact vulnerabilities based on business impact.
- Analytics and reporting solutions for Risk Management: Performance Analytics Solutions contain preconfigured dashboards. These dashboards contain actionable data visualizations that help you improve your business processes and practices.

## GRC Risk Workspace

Starting with version 13.0.5, the GRC Risk Workspace provides a new and simplified user experience with a single-pane view. In the workspace, you can perform the same functions as the classic environment, but with more intuitive functionality. These functions include risk assessments, risk events processing, and so on.

The Risk Workspace is highly configurable and role-driven. Being role-driven means that the Risk Workspace is customized or unique for each user or role in your organization. In the workspace, different users with specific roles can perform different functions and have views that differ from each other. The workspace also reduces the number of apps that the users must install to utilize the Risk Management application. For example, if you want to manage your IT risks, you must install only one application. The workspace makes the management and installations of apps easier. To use the Risk Workspace, you must install and activate the **GRC: Risk Management workspace** (com.sn_risk_workspace) plugin.

The starting point in the Risk Workspace is the Home page  .

The Home pages show you the complete view of the risk status across your organization. Some of the key items that you can see are the key risk indicator (KRI) breaches, the risk heatmaps, the risk classification and breakdown, entities at the highest risk and so on.

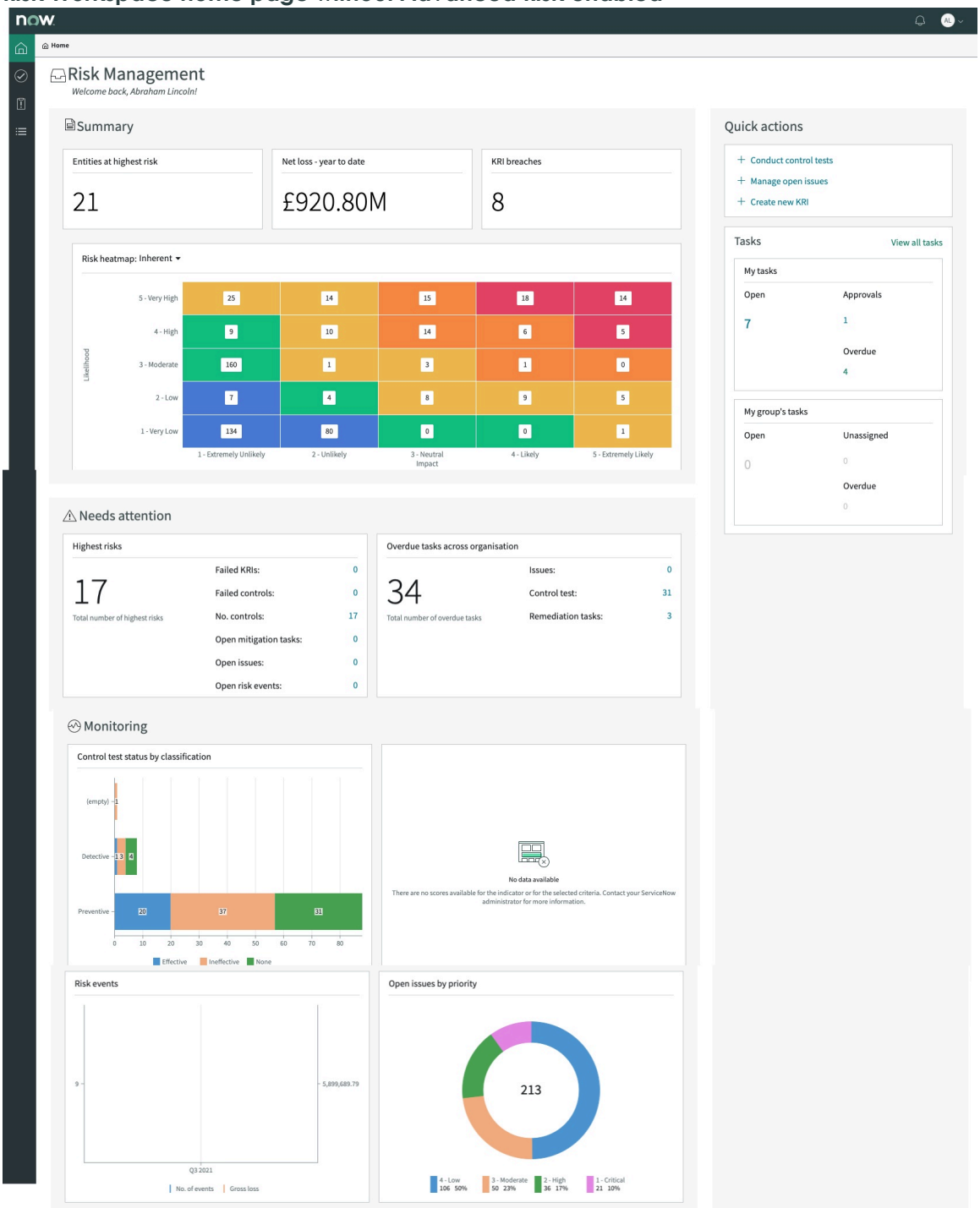
The Home page offers the following benefits:

- Provides a different view for each role.
- Is designed for the specific responsibilities of each role.
- Shows the day-to-day tasks for each role depending on the user. For example, the Home page for an Operational Risk Manager differs from that of the Home page of the IT Risk Manager.
- Displays the key tasks assigned to you and your group. This makes it easier to get a complete view of your actionable tasks. For more information on the new user experience for Advanced Risk Assessments, see Advanced Risk Assessments in the Risk Workspace.
- Shows the risk profile for the top entities. This consolidated view enables easier reporting.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Enables customization to suit your needs. For example, you can configure your own color codes for heatmaps and reports. For more information, see Operational risk heatmap for Advanced Risk Assessment in the Risk Workspace
- Provides quick links for performing key tasks such as scheduling risk assessments, creating new key risk indicators, and so on.
- Provides data in a way that you can click and view the details.
- Shows the classic risk assessment scores if the Advanced Risk application is not enabled.

### Risk Workspace home page without Advanced Risk enabled




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Roles and user enhancements in the Risk Workspace

The roles for the Risk Workspace are the Operational Risk Manager and IT Risk Manager. See the following sections for the description of each role, its responsibilities, and its tasks.

**Note:** Because the roles in your organization might be different from what is presented here, use these roles as references or models.

Multiple enhancements have also been made to the user experience in the Risk Workspace. Each enhancement is described in detail in the subsequent sections.

### Risk Workspace for the operational risk manager

Operational risk managers manage operational risks such as losses due to errors, breaches, or damages that are caused by people, internal processes, systems, or external events. Operational risks range from the small, such as the risk of loss due to minor human errors, to the large, such as the risk of bankruptcy due to serious fraud.

## Operational risk manager

Operational risk managers are a part of the operational risk team that manages the risk posture of the organization. Risk posture is the current risk profile for a company. As an operational risk manager, you must perform the following tasks.

Define the operational risk framework

Effectively manage the operational risks of an organization by defining a robust risk management framework. This framework helps to identify risks and to define the control framework to mitigate those risks. A risk management framework consists of the following components:

- Risk identification
- Risk measurement or scoring
- Risk mitigation
- Risk reporting and monitoring

Set up libraries

Set up comprehensive libraries by doing the following:

- Creating risk statements: A risk statement is used to record a risk in a way that everyone can reach a common agreement on its severity or relative priority.
- Creating control objectives: A control objective defines the aim or purpose of risk-mitigating controls. These controls need continuous monitoring.
- Defining entity classes, entity types, and entities: For more information on entities, see Understanding entities.
- Defining the upstream and downstream entities.

The first step is to set up risk statements so that your team has a specific idea of the risk. For example, simply calling a risk as a cybersecurity risk is not specific. Cybersecurity risks could mean different things to different people. Therefore, a common statement to define cybersecurity is created as a risk statement. To create risk statements and their hierarchy, clearly define the risk impact, the assets at risk, and the source of risk. By defining the risk statements and creating their hierarchy, you can ensure that the risk scores are aggregated thus giving the complete risk status.

Conduct risk assessments on a periodic basis

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Perform the annual risk assessments according to your organization's policies. Also, ensure that the risk register is updated and accurate. Create risk assessment scopes and schedule assessments. To learn more about risk registers, see Risk register in the Risk Workspace.

Record and monitor risk events

Risk events are potential or actual financial and non-financial losses, near misses, and gains that occur within an organization. To effectively manage risks, it is essential to monitor risk events, perform a root-cause analysis, and track the remedial tasks. Organizations use risk events to understand their losses and analyze areas of improvement to reduce further losses. You must maintain the loss event register to capture complete event information and to suggest additional controls to mitigate risks in the future.

Define key risk indicators

Monitor the risk posture of your enterprise on a continuous basis. Continuous monitoring of risks and controls involves identifying and creating key risk and control indicators. Supporting information can be collected for those indicators through automatic data collection or manual tasks. Indicator results are then used to create issues for controls, signal a change in the risk posture, and to provide supporting information for audit activities and control testing. If the indicator thresholds are breached, you must escalate to the respective stakeholders.

Manage issues and incidents

An issue is created when there is a change in the environment, process, or system that poses a threat. An issue requires action to prevent an incident or loss. An incident is a successful outcome or event with a negative impact. As the operational risk manager, you can view, create, and manage issues and incidents. Ensure tracking, proper closure, remediation, and monitoring of issues and incidents.

Communicate the operational risk posture

Define dashboards to report data effectively and accurately. You must create the required reports which can be shared with the executives and the head of the operational risk team. The reports and dashboards ensure that the aggregated assessment results across the organization help to identify the top operational risks for the enterprise.

The following table lists the key tasks that you perform in your role as an operational risk manager.

**Tasks of an operational risk manager**

| Activity | Task |
| --- | --- |
| Define the operational risk framework | • Create a risk statement<br>• Create a risk framework in the Risk Workspace<br>• Associate a risk statement with a control objective in the Risk Workspace |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

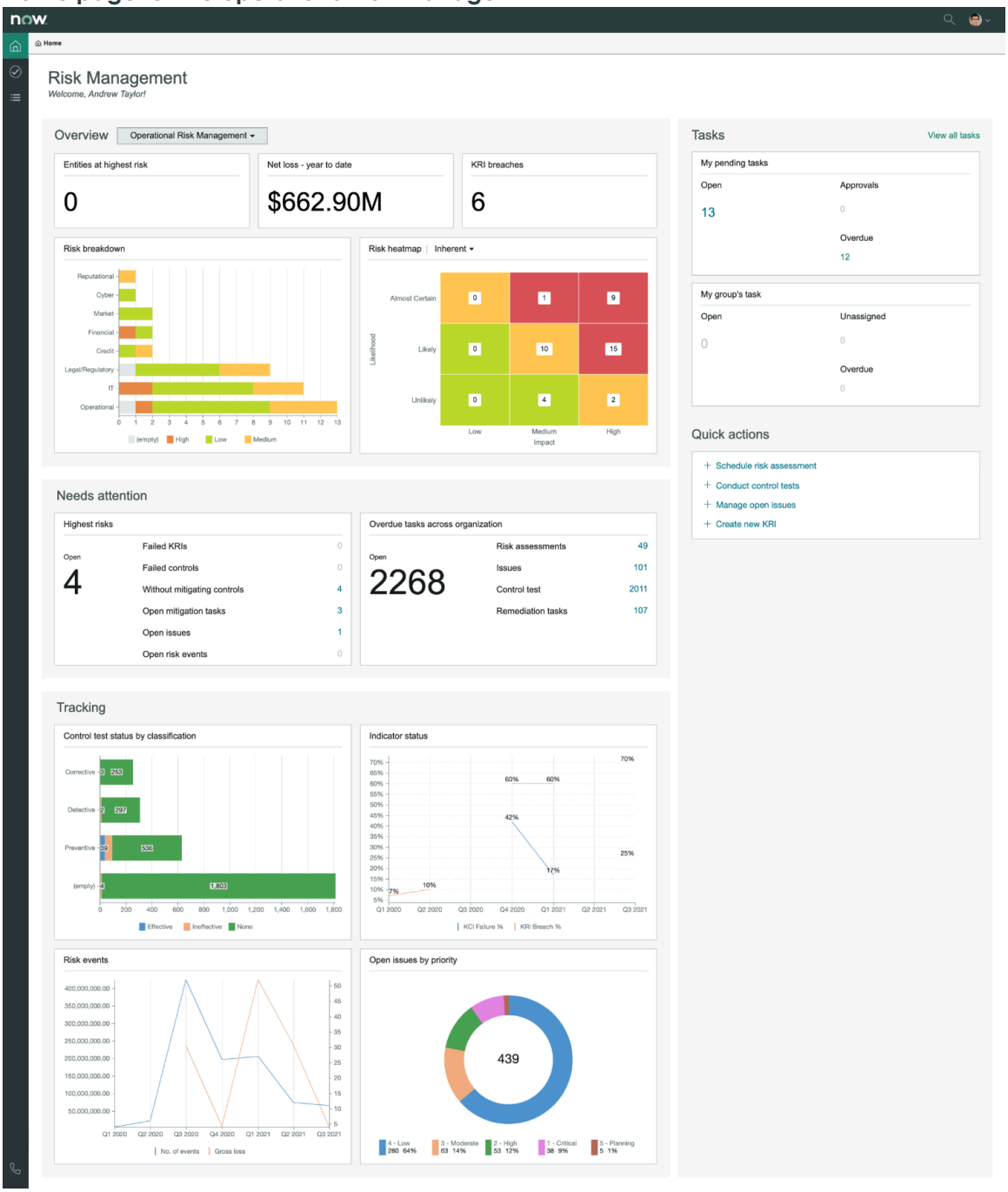
**Tasks of an operational risk manager (continued)**

| Activity | Task |
| --- | --- |
| Communicate the operational risk posture | • Operational risk heatmap for Advanced Risk Assessment in the Risk Workspace<br>• Risk heatmap for classic risk assessment |
| Monitor the critical incidents and issues | View, create, and manage issues |
| Define the key risk indicators | Risk indicators, control indicators, and indicator templates |
| Conduct the annual risk assessment process | • Configure a risk assessment methodology<br>• Create factors<br>• Create risk assessment scopes<br>• Schedule risk assessments in the Risk Workspace<br>• Perform advanced risk assessment in the Risk Workspace |
| Facilitate recording and learning from loss events | • Manage risk events<br>• Create a risk event in the Risk Workspace<br>• Analyze a risk event in the Risk Workspace<br>• Create a risk event entry in the Risk Workspace |
| Create aggregated risk reports | Reports in the Risk Management application |

The following image shows the view for the operational risk manager.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Home page for the operational risk manager




Related topics

Roles installed with the GRC Risk Workspace

### Risk Workspace for the business operational risk manager

Business operational risk managers are the first lines of defense for each individual line of business. They are responsible to manage the risk posture of their specific business units.

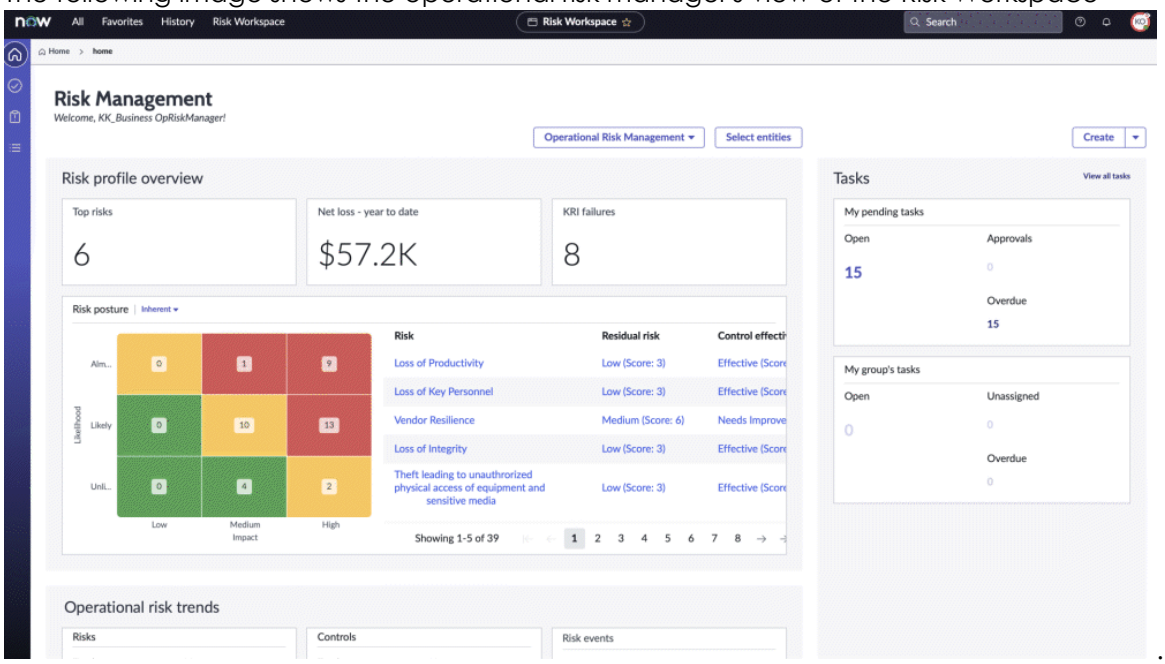
A business operational risk manager has the role sn_risk_workspace.business_op_risk_manager. As a business operational risk manager, you can do the following in your workspace.

- Filter the appropriate risk assessment methodology to view the relevant data.
- View the performance of your entity by viewing the number of top risks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- View the number of key risk indicators that have failed.
- The net loss beginning the first day of the current calendar year or fiscal year up to the current date.
- Create risks, risk events, and indicators.
- View the operational risk trends such as the not assessed risks and new risks identified in the last 30 days.
- View the risks by category.
- View the control status, the number of new controls, and the number of controls not attested.
- View the number of overdue issues and the number of new issues.

The following image shows the operational risk manager's view of the Risk Workspace




To view the risk assessments for the top risks for your entities, click the **Top risks** card.

The heatmap on the workspace gives critical insights into the risks when you select each tile of the heatmap. You can use the filter on the heatmap to view either the inherent risk posture or the residual risk posture. For more information, see Risk heatmap workbench.

### Risk Workspace for the IT risk manager

Information technology or IT risk is any threat to your business data and critical systems. It is the risk associated with using and operating IT within an organization. An IT risk manager is the primary person responsible for establishing and maintaining the organization-wide IT risk management program.

IT risks vary in nature. It is important to be aware of all the different types of IT risks potentially affecting your business. An IT risk manager works with various stakeholders to ensure that IT risks are managed within the risk appetite of the organization. To facilitate risk assessments for IT risk managers, a preconfigured risk assessment methodology (RAM) is also provided by default. IT risk managers can use this RAM or make modifications to it according to their requirements.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

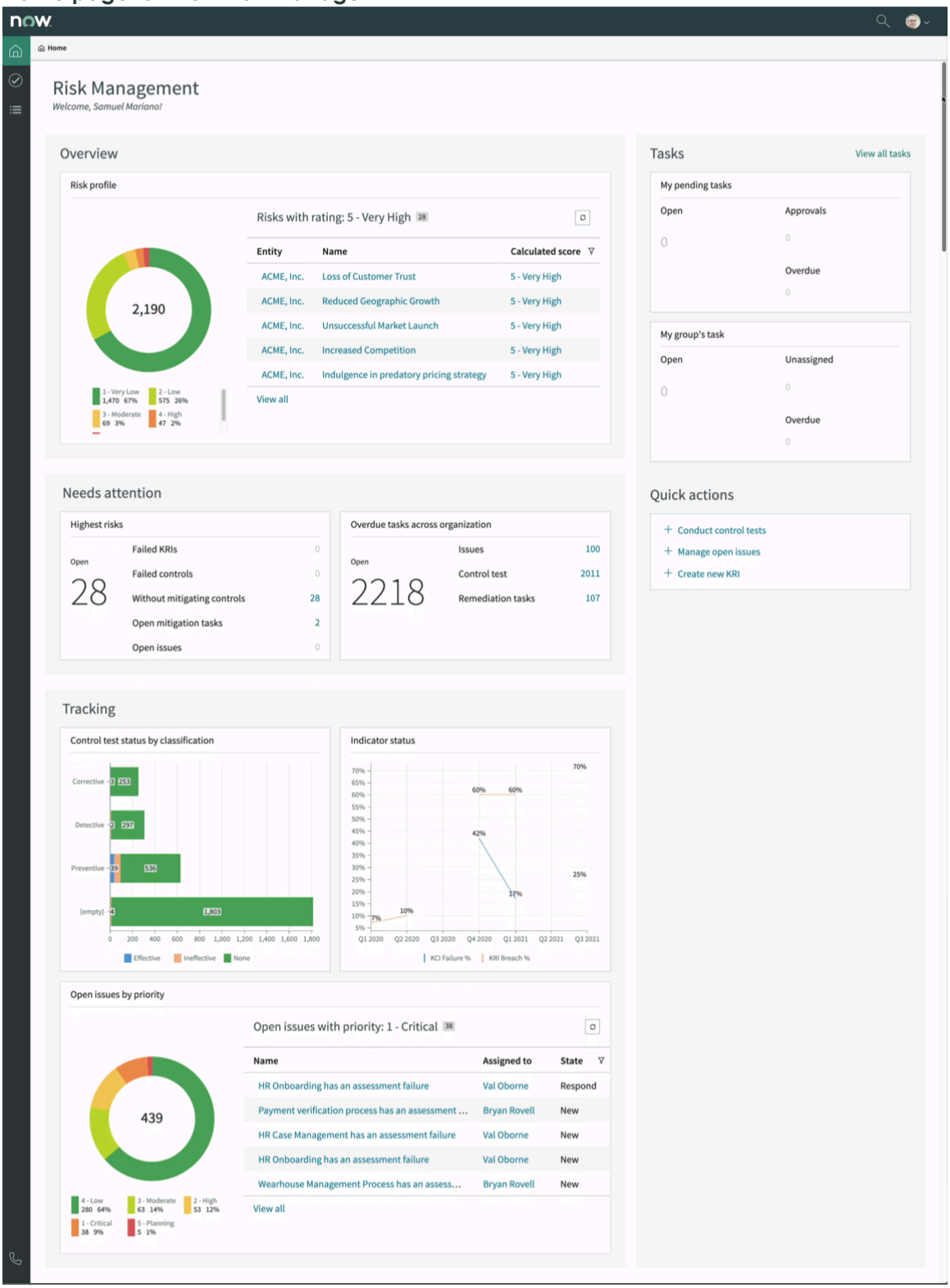
**Tasks of an IT risk manager**

| Activity | Task |
| --- | --- |
| Identify risks using a workflow. | Workflow for risk identification in the Risk Workspace. |
| Identify, assess, mitigate, and monitor all IT risks. | • Create a risk assessment scope in the Risk Workspace.<br>• Schedule risk assessments in the Risk Workspace. |
| Manage IT risk remediation actions and define the action plan. | Managing risk responses. |
| Communicate the IT risk posture. | Risk heatmap for classic risk assessment. |
| Define the key risk and control indicators. | Risk indicators, control indicators, and indicator templates |
| Create control test plans | Create a test plan in Risk Workspace |

The following image shows the view for the IT risk manager.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Home page for the IT risk manager




## User experience enhancements in the Risk Workspace

In the new workspace, several enhancements have been made to ease the way you perform your daily tasks. The user experience enhancements are useful for new GRC users or users who do not have the complete experience of GRC.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Views of the Risk Workspace

The new workspace offers the following views for the users.

List view

The list view shows a simplified list of all the modules. You can access the list view by clicking the List icon (  ).

Record view

The record view provides detailed information about any record. For example, in the risk statement form, you can view the complete hierarchy including the parent and children of the risk statement. This view provides the complete details including important information such as open indicator breaches, open issues, open risk events and so on.

## Miscellaneous user experience improvements

Overview pages of records

The Overview tab of each record provides you a summary of all the information you need in a single view. For example, for a risk record you can see KRI breaches, the controls failures, the number of issues open, the open indicator tasks, the number of risks assessed and so on.

Contextual side panel for records

The Contextual side panel of a record provides detailed related information for the records. For example, for a risk, you can see the parent and child hierarchy. You can display and close the Contextual side panel by clicking the reference icon (  ).

Tasks

Tasks is a centralized task inbox that shows your tasks and your group's tasks. You can access your tasks by clicking the Tasks icon (  ).

360° relationship view

The 360° view feature enables you to view the relationships between a selected record and related objects, such as controls, risks, and entity types. The 360° view also enables you to interact with all records displayed. For more information, refer to 360° Relationship Visualization.

Breadcrumb navigation

The breadcrumb style navigation provides a browser path to navigate a hierarchy of linked pages with related content. The breadcrumb style navigation provides a digital trail from the user's starting point to the current content, with the ability to navigate to each link. For more information, refer to Breadcrumb navigation

Consolidated issues page

The comprehensive issue management page shows you a detailed status of your issues. For example, you can see overdue issues, issues approaching the overdue date, issues by priority and so on. You can also see the issues assigned to you and your group. This feature makes issue tracking easy. You can access your issues by clicking the Issue landing page icon (  ). For more information, refer to Issue management in the Risk Workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

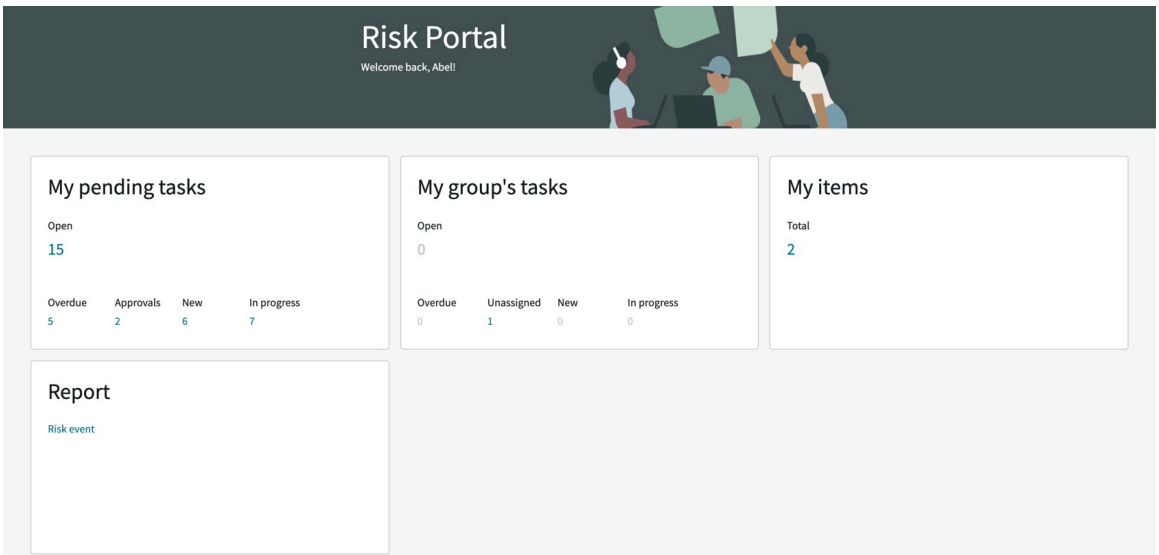
### GRC Risk Portal

The GRC Risk Portal is a simplified interface that enables the GRC business users to view their tasks and their group's tasks. The Risk Portal also enables users to report risk events.

To access the Risk Portal, navigate to **Risk** > **Risk Portal**. To use this portal, you must have the sn_grc.business_user role. On the Risk Portal you can do the following:

- **My pending tasks**: View the tasks that are pending and are assigned to you. For example, if you have a risk assessment assigned to you, you can launch it from the Risk Portal.
- **My group's tasks**: View the tasks assigned to your group.
- **My items**: View the requests you have raised. For example, issues, policy exceptions, remediation tasks and so on.
- **Report**: Report a risk event. To see how you can report a risk event from the Risk Portal see, Report a risk event from the Risk Portal

#### Risk Portal




### Advanced Risk Assessments in the Risk Workspace

The Risk Workspace offers an enhanced and a simplified user experience for users to perform Advanced Risk Assessments. You can quickly access the risk assessments assigned to you or your group from the GRC Risk Portal or the Risk Workspace.

With the new Risk Workspace, your risk assessments are more intuitive with more data readily available for you to refer for every assessment that you perform in the risk assessment instance. As an operational risk manager, when you use Advanced Risk Assessments, on the Home page, in the **Risk Summary** field,you have a filter available to select your risk assessment methodology. For example, you can select the risk assessment methodology that shows you the operational risks assessed. For more information on risk assessment methodologies, see Advanced Risk Assessment.

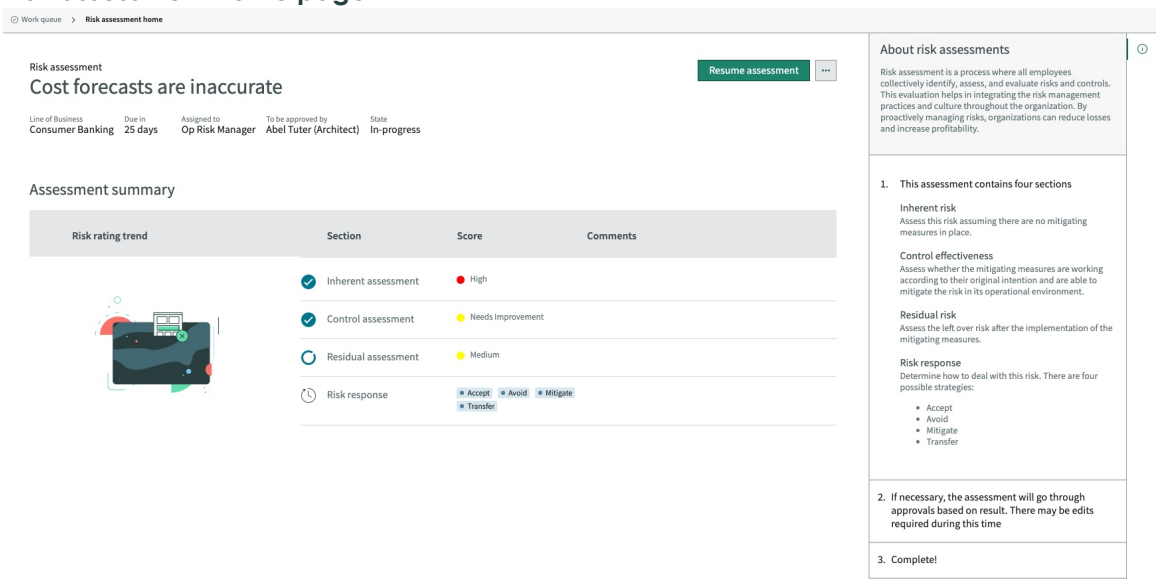
For a new user to understand risk assessments, a Contextual side panel is provided with an explanation about the assessment sections. While a default explanation and a brief training are provided, you can also configure the system to show your training content related to risk assessments. If you do not want to keep the side panel training information open, you can also close it using the information icon.

At a glance, the risk assessment home page shows you the entity being assessed, the due date for the assessment, the person the assessment is assigned to, the approver, and the risk

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

description. The home page also shows the results of the risk assessment and the selected risk response strategies.

**Risk assessment home page**



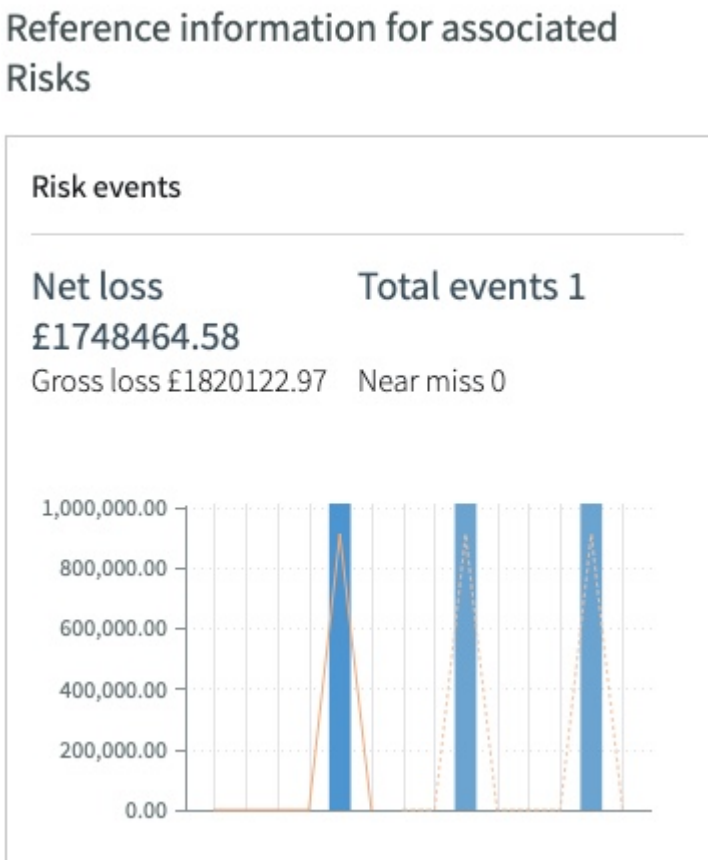

Some of the major enhancements for Advanced Risk Assessments in the Risk Workspace are as follows:

## View reference information for associated risks and controls

The Contextual side panel shows the reference information for associated risks and controls. The graphical representations can be clicked to get detailed information about the risk events, issues, indicator breaches and so on. The reference information shows the following:

- Risk events graph that displays the gross loss and the net loss of the aggregated risk events for that particular risk. This graph also displays the forecasts of the losses.
- Percentage of key indicator breaches for every quarter.
- Percentage of control indicator failure graph. When performing a control assessment, you can refer to the control test results, indicator failures, and so on
- Number of open issues with their severity. You can also create issues by clicking the plus icon.

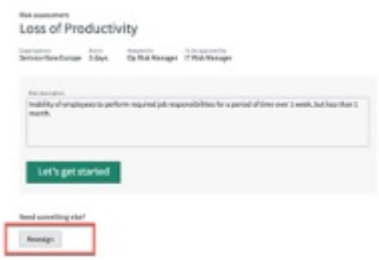
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## View factor guidance

In the workspace, while responding to factors, you can quickly view the guidance by clicking the Show guidance icon . This ability saves your time as you can view the guidance and understand the factor while responding.

## Reassign assessments

If you are assigned a risk assessment that must be assessed by another user, you can reassign the assessment from the risk assessment home page. In case there are two users with the same name, you have the ability to view their email addresses while reassigning the assessment. This ability prevents users from assigning the assessment to the wrong users. 


## View factor weighting information

As a first line risk assessor, you may need to view the qualitative weight, the qualitative score, and the quantitative score of a factor. You can easily access this information by clicking **Overall rating**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Perform advanced risk assessment in the Risk Workspace

## Advanced Risk Assessment

Use the ServiceNow® Governance, Risk, and Compliance (GRC) Advanced Risk Assessment feature to create an integrated risk platform. This integrated platform supports various kinds of risk assessment methodologies. It enables you to integrate risk assessment as part of your overall decision-making process.

Advanced Risk Assessment offers the following benefits:

- Digitizes the complete risk management life cycle, including risk identification, risk analysis, risk evaluation, risk treatment, and monitoring.
- Customizes the risk assessment process based on the unique needs of your organization. This customization includes configuring the assessment criteria, the context, and the overall risk scoring logic.
- Supports both qualitative and quantitative risk assessment methods.
- Automatically aggregates the bottom-up risk assessment scores across the risk.
- Embeds the risk assessment process in the workspace for first-line users. This embedding helps users make informed decisions based on risks that are associated with actions.

**Note:** To know if your current license entitles you to Advanced Risk Assessments, contact ServiceNow.

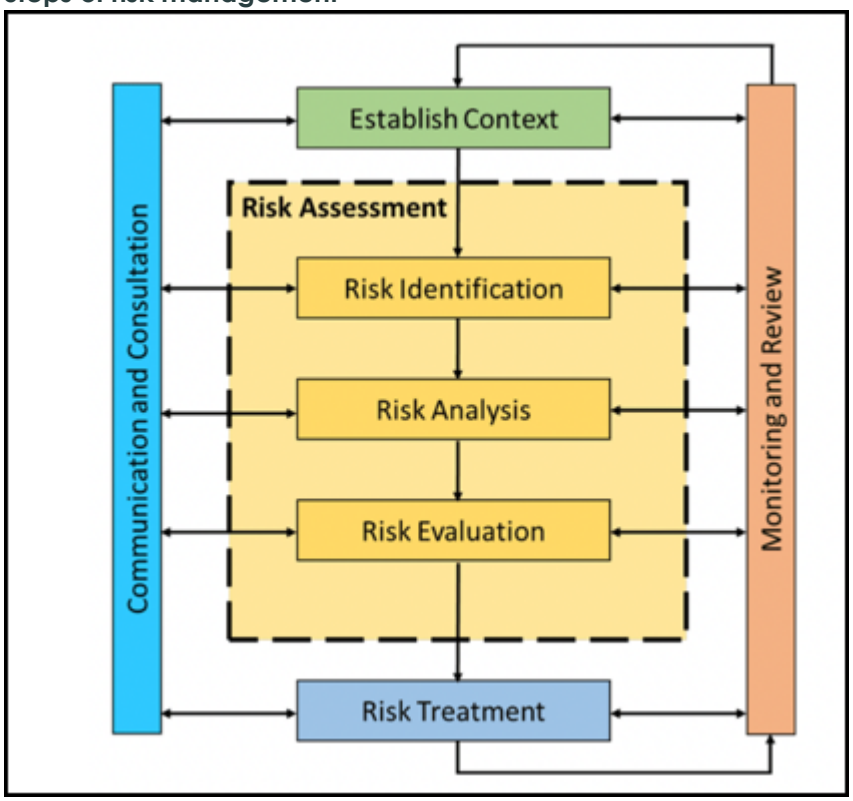
## Steps of risk assessment

Before understanding Advanced Risk Assessment in detail, it is important to understand the key steps of risk management:

1. Risk identification: Find an uncertainty or risk that might prevent your organization from achieving its objectives.
2. Risk analysis: Understand the cause and consequence of the risk.
3. Risk evaluation: To determine if additional action is required, compare the results of the risk analysis with the established risk criteria.
4. Risk treatment: Define an action plan to address the risk.
5. Risk monitoring: Track the risk posture of the organization and communicate it to relevant stakeholders.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Steps of risk management**




Risk assessment consists of risk identification, risk analysis, and risk evaluation. Advanced risk assessment is performed based on factors or questions and their responses. It can be performed for an entity such as an organization. To use advanced risk assessment, you must enable the **Migrate to Advanced Risk Assessments** property located under the Administration module. The assessor and approver for the risk assessment must have the sn_grc.business_user role. Advanced risk assessment enables you to do a detailed assessment of the risks where the inherent risks, mitigating controls, and residual risks are assessed. If you don't have the complete GRC setup for entities, risk statements, controls, and so on, then you can still assess the risks on any ServiceNow record or object. An example of object assessment is assessing change management. During risk assessment, the following risks are assessed.

- Inherent risks: Inherent risks are risks that don't have controls. For example, driving at a high speed on a highway is inherently more of a risk than driving at a moderate speed. The score of this inherent risk is derived by multiplying the impact of the risk and the likelihood of the risk.
- Control effectiveness: Controls can mitigate the impact or likelihood of a risk. For example, highways have speed limit monitors. If a risk materializes, the controls mitigate the impact. Controls can be preventive, detective, or corrective.
  - Preventive controls are designed to prevent errors, inaccuracies, or fraud before these issues occur.
  - Detective controls are intended to discover the existence of errors, inaccuracies, or fraud.
  - Corrective controls are designed to correct errors or irregularities that have been detected.
- Residual risks: Residual risks are the leftover risks that remain after the implementation of controls. For example, despite the safety measures in place, if there's still an accident, then the damage caused by the accident is a residual risk. A residual risk score can be calculated using any of the following methods:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- A matrix between inherent and residual effectiveness.
- A mathematical formula such as the inherent score minus the control score.
- Answers to factors.

- Target risks: Target risks are the desired risk an organization want to achieve in the future. By evaluating the desired level of likelihood and impact of identified risks, organizations can establish target risk levels for each risk. For example, when assessing a risk, you consider various aspects such as inherent risk, the effectiveness of controls, and residual risks. However, it's equally important to capture the desired risk level that will be attained after your risk response is implemented. The target risk represents the optimum level of risk that you aim to achieve after your action plan is successfully executed. It enables you to measure the benefits your organization gets in relation to the cost of implementing those actions.

### Workflow of Advanced Risk Assessment

To use Advanced Risk Assessment, you must set up the risk assessment methodology (RAM), define the assessment scope, and perform the assessment.

Before using Advanced Risk Assessment, different users must perform different setup tasks. These steps define the workflow of the assessment.

1. Set up the risk assessment methodology (RAM): A risk administrator with the sn_risk.admin role sets up the system. The administrator does the following:
   - Identification: Identifies if a risk or an object is being assessed.
   - Assessment: Determines how to assess the issue, such as with assessment criteria, risk scoring, or reporting preferences.

   For more information, see Configure a risk assessment methodology.
2. Define the risk assessment scope: After the RAM is defined, the entity owner defines and identifies the following:
   - The relevant risks for the entity.
   - The assessors and approvers for those assessments.
   - Periodicity of those risk assessments.

   For more information, see Create a risk assessment scope and initiate assessments or Create a risk assessment scope in the Risk Workspace.
3. Perform risk assessment: The risk assessor with the sn_grc. business_user role performs the following assessment tasks.
   - Assesses the inherent risks and the effectiveness of mitigating controls.
   - Reviews the residual risk and defines the risk treatment plan.
   - Perform a target risk assessment to define your desired future risk level.
   - Triggers the review and approval workflow.

   For more information, see Perform advanced risk assessment in the Risk Workspace.
4. Monitor the assessments: After the risk assessment is approved, the assessment moves to the Monitor state. The risks assessed in the risk assessment must be monitored especially if it contains automated factors. Automated factors or questions that automatically fetch data from any of the data sources have ever-evolving risk ratings. Therefore, a risk which may currently have a low rating might have a higher rating later. This makes it imperative to monitor a completed assessment to reduce threats to your organization.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Factors in Advanced Risk Assessment

Factors are questions that you can use to analyze risks. Factors appear on a risk assessment instance.

Factors are questions that appear during the risk assessment. To use Advanced Risk Assessment, you must first define these factors and configure a risk assessment methodology (RAM). For more information on RAMs, see Configure a risk assessment methodology. Each factor or question has a response. There are different types of factors:

- Manual factor: A factor that requires human input. The response is a manual response. An example is your name.
- Automated factor: A factor whose response is automatically calculated. An example is the temperature in your city today. The information is fetched from external sources.
- Scripted automated factors: A factor that is used to write scripts.
- Group factor: A set of factors that are grouped logically.

These factor types are explained more in the following sections. After you define the factors and publish them, you can configure a RAM and associate the factors to the assessment types within the RAM. The RAM forms the basis of the risk assessment. Publish each of the selected assessment types, and then publish the RAM. Users with the sn_risk.user role can select the assessment types for which the assessment must be performed.

Your risk assessment instance is then created. Its properties depend on the assessment types and options that you selected for your RAM. The risk assessment instance is where the risk assessor evaluates the risks. As a question, a factor can be used in multiple assessment types. For example, a question such as "What is the probability of a building getting flooded?" can be a part of either an inherent assessment or a residual assessment after the control effectiveness assessment.

**Note:** A factor can be used in multiple assessment types, but it can be used in only one RAM. A factor that is created and used in one RAM cannot be reused in other RAMs.

## Types of factor contributions

An assessor provides responses to factors. Risk assessors can contribute to factors in the following ways:

- Qualitative: Losses are in the form of subjective terms such as high, medium, and low. The losses can also be in the form of a numerical score that is converted into a rating.
- Quantitative: Losses are in a numerical form. They can be incurred from a risk in monetary terms. They contribute to the inherent Annual Loss Expectancy (ALE).
- Both: Losses have both a qualitative risk rating and a quantitative dollar value. These ratings are also called semi-quantitative.

For more information on understanding qualitative, quantitative, and semi-quantitative ratings, see Types of risk rating methodologies

## Manual factors

In a risk assessment, questions that need human responses from the respondents are called manual factors. In manual factors, the response is subjective and difficult to classify. Some questions require human intelligence and assessment. Therefore, a manual factor is a subjective assessment of a person's view. Examples of manual factors are reputational

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

impact, expected speed of onset, and so on. In manual factors, users can provide the following types of responses:

- Text: A descriptive answer. For example, feedback. This choice does not contribute toward the risk score calculation.
- Choice: User-defined choices to the questions in the assessment. For example, users can select risk ratings from low, medium, or high.
- Number: A numeric value. For example, the number of open issues.
- Currency: An amount in the local currency of the user. For example, the financial impact of a certain risk.
- Percentage: A percentage value for the questions in the assessment. For example, the percentage of employees satisfied with the organization strategies.

## Group factors

When factors are grouped logically, they are called group factors. A group factor's score depends on the responses of the corresponding manual factors. For example, organizations are affected from financial risks and non-financial risks. You can create some factors for financial risks, and other factors for non-financial risks. You can combine these two sets of factors into a single group factor called Overall Impact. Like manual factors, group factors can contribute either to a numerical risk score that is converted to a qualitative contribution, or to the ALE values as a quantitative contribution.

## Automated factors

Automated factors automatically fetch the latest data, during an assessment, from any of the data sources such as tables or database views. Automated factors help to automate the risk assessment process. They do not rely on manual inputs, and thus reduce subjectivity. For example, a risk assessor wants to perform an assessment for different locations. One of the automated factors is the political condition of a country, and this information is publicly available on a website. Because this data does not reside within ServiceNow, the assessor can use automated factors to fetch the data. Some other examples of automated factors are the following:

- The number of employees on a project.
- The revenue of a business unit.
- The business criticality of a process.

## Scripted automated factors

Automated scripted factors are used to write scripts. The scripts fetch the data from either ServiceNow records or from external sources. Scripted automated factors automatically provide the responses for factors during risk assessment.

The following use cases demonstrate an example of how you can model scripted factors. For example, if you want to use the results from the compliance function to assess the mitigation effectiveness of the controls, there are two ways for assessing the controls:

- Individual assessment of controls
- Control environment assessment.

In the individual assessment of controls, each control is separately assessed. To understand control assessment in the context of scripted factors, consider the example of money laundering as a risk. In this example, the control effectiveness is assessed based on the percentage of the failed controls. The values of the failed controls are then transformed into

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a rating to calculate the control effectiveness of that control. For example, the risk of money laundering has three mitigating controls:

- Employee training
- Internal audit on employees
- Customer due diligence

Assume that you have defined the control effectiveness criteria in the following manner:

| Control Design Effectiveness Failure | Control Effectiveness |
|---|---|
| 0%-30% | Effective |
| 30%-60% | Needs improvement |
| > 60% | Ineffective |

Now, assume that out of the three controls, one control passed and two controls failed. The failure of two controls translates into a 66.67% failure rate. Based on the transformation and based on the previous table, the control effectiveness rating is ineffective. You can use this defined script to automate the response to the factor to assess the risk of money laundering.

As for control environment assessment, you can assess the complete control environment instead of assessing each control individually. To understand control environment assessment, consider the following example. Assume that you want to assess the control environment based on two aspects: design effectiveness and operating effectiveness. To calculate the design effectiveness, you can fetch the related controls that are related to the risk of money laundering. You can then look at the test results to understand how many of the controls had failed. Assume that you have defined the control effectiveness criteria in the following manner:

| Control Design Effectiveness Failure | Control Effectiveness |
|---|---|
| 0%-30% | Effective |
| 30%-60% | Needs improvement |
| > 60% | Ineffective |

Now, assume that two controls failed and one control passed. Thus, the control design effectiveness failure rate is 33.33%. Based on the previous table, this low value of 33.33% means that the control design needs improvement. This response can be automatically scripted in the automated scripted factor because it does not need any human calculation or intervention.

### Types of risk rating methodologies

Risks are scored during an assessment and then a rating is derived. Ratings are of three kinds: qualitative, semi-quantitative, and quantitative.

## Qualitative rating

Qualitative risk assessments rely on the assessor's perceptions of the probability and impact of a risk. If the method is purely qualitative, then the ratings are based on the list values such as high, medium, or low. In this case, the risk scores do not roll up. Because this method has minimal mathematical dependency, qualitative risk assessment is easy and quick to perform. This method also enables an organization to take advantage of the assessor's experienced knowledge of the process or asset that is being assessed. Users who are new to risk assessments usually use this kind of rating.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following figure shows an example of qualitative rating.

**Qualitative risk assessment**

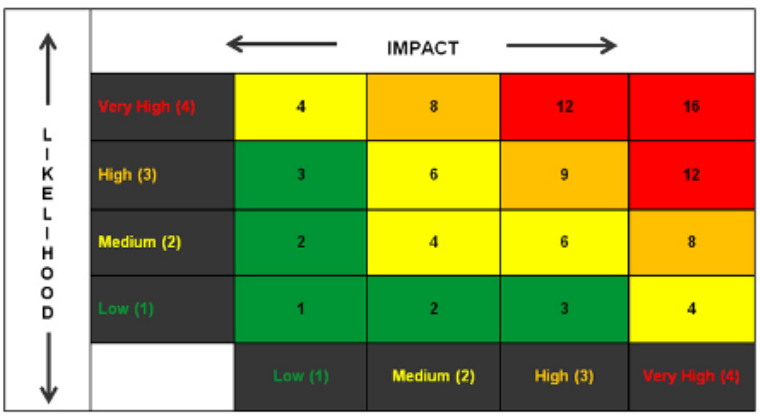
| | | Impact | | |
|---|---|---|---|---|
| | | Low | Medium | High |
| Probability | Low | Low Risk | Low Risk | Medium Risk |
| | Medium | Low Risk | Medium Risk | High Risk |
| | High | Medium Risk | High Risk | High Risk |

## Semi-quantitative rating

In a semi-quantitative rating, the qualitative ratings also have a corresponding numerical scale. For example, if the quantitative risk score is between 0-10, then the qualitative rating is low. Users who use this type of rating are not new to risk assessments. Most users belong to this category. In this category, the risk scores roll up and the risk appetite is qualitative in nature.

The following figure shows an example of semi-quantitative rating.

**Semi-quantitative risk rating**




| Risk Score | Rating |
|---|---|
| 0 – 3 | Low |
| 4 – 6 | Medium |
| 6 – 9 | High |
| 10 – 16 | Very High |

## Quantitative rating

A quantitative risk assessment focuses on data that is fact-based, measurable, and highly mathematical. In a quantitative risk rating that uses advanced simulation techniques, the risk is quantified in purely numerical terms. In this category, the risk appetite is quantitative in nature.

### Transformation criteria

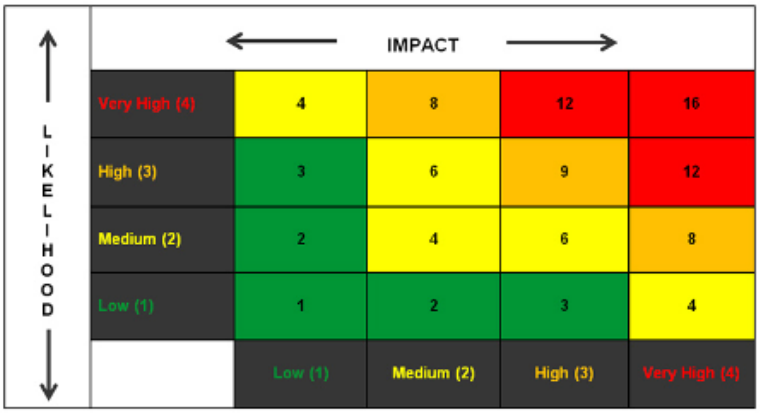
After the risk scores are calculated, you can transform the scores into a rating and then easily report the ratings to senior management and to other stakeholders.

Scores are transformed into a rating because ratings provide clear meaning and interpretation for the scores. The transformation of risk scores is done using transformation criteria. You can define the transformation criteria based on your requirements. For example, you can define that a risk score between 80-100 is a high risk.

The following figure shows an example of the rating transformation criteria.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Rating transformation Criteria




| Risk Score | Rating |
|---|---|
| 0 – 3 | Low |
| 4 – 6 | Medium |
| 6 – 9 | High |
| 10 – 16 | Very High |

### Any object assessment using Advanced Risk Assessment

If you don't have the complete GRC setup for entities, risk statements, controls, and so on, even then, you can still assess the risks on any ServiceNow record or object. An example of object assessment is assessing change management or assessing a citation.

Any object assessment is used to perform risk assessment on any ServiceNow record. To perform a risk assessment, a prior knowledge of risk is not necessary. Using the assessment results, risk managers can quickly analyze the risks associated with their project or application.

Any object assessment can be performed in the following ways:

- Ad hoc: In an ad hoc based risk assessment, users can perform the assessment through a UI action.
- Event driven: In an event driven risk assessment, a user can perform the risk assessment based on some event.

To perform any object assessment, you must create a risk assessment methodology with **Object** as the context and then select the relevant table.

**Note:** You cannot assess your controls if you perform the risk assessment for an object. The reason for this limitation is that controls are associated to either an entity or a risk. Also, the risk response workflow is not available for the assessment of an object.

After you generate an assessment, you can add a related list in the object in which you can see the list of assessments. For more information on how to configure any object assessment for an object and create the **Assess risk** button, see the Perform any object assessment [KB0826429] article in the Now Support Knowledge Base.

For information on how to configure any object assessment in the Risk Workspace, refer to the Any object integration in workspace [KB0961251] article in the Now Support Knowledge Base.

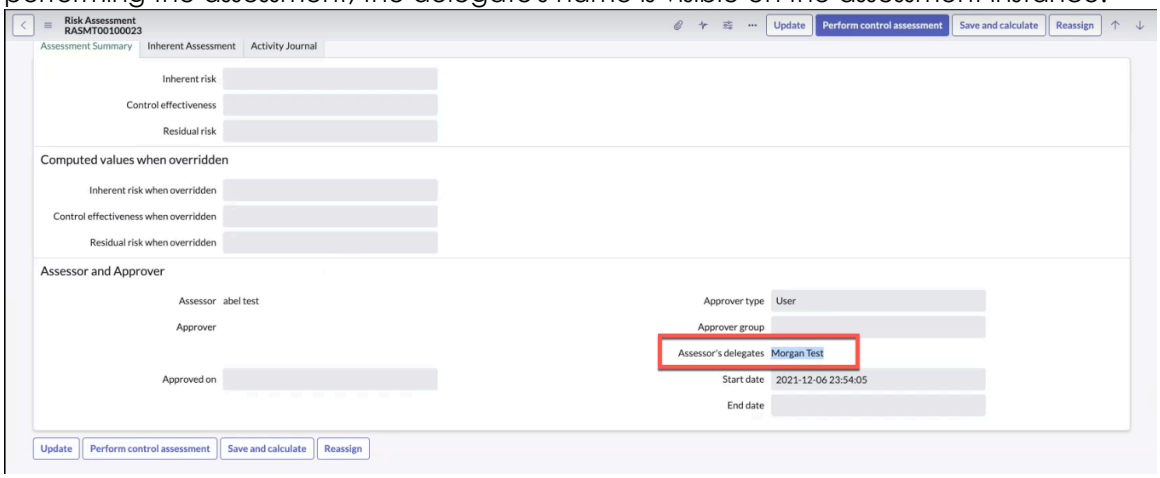
**Note:** You must log in to Now Support to view the articles.

### Delegation of risk assessment

If a risk assessor is unavailable to perform a risk assessment, the assessor can appoint a delegate to perform the risk assessment for a specified time period. The Now Platform enables you to appoint your delegates.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Delegation is the assignment of authority to another person to perform specific activities. It is a process of entrusting work to another person. In the context of risk assessments, at times, it may happen that the assigned assessor for a risk assessment is unavailable to perform their risk assessments. In such a scenario, the assessor can assign another user as a delegate and the delegate can perform the risk assessment on behalf of the original assessor for a specified time period. A delegate can perform the risk assessment from the Risk Workspace and the Risk Portal. A delegate also receives a copy of all the system notifications that are sent to the original assessor. Once the delegate starts performing the assessment, the delegate's name is visible on the assessment instance.




As a risk assessor, to understand how you can assign a delegate, refer to Configure a delegate for your tasks.

To delegate tasks to another user, configure your user profile form to display the Delegates related list. For details, refer to Add the Delegates related list.

It is important to note the following points when you assign a delegate.

- The ability to assign a delegate is only available to perform an assessment. You cannot assign a delegate for approving a risk assessment.
- After a delegate is assigned an assessment, the assessment shows the names of the original assessor as well as the delegate.
- You can only assign an individual user as a delegate and not a group.
- A delegate must have the sn_risk_advanced.ara_assessor role to perform risk-based assessment.
- A delegate must have the sn_risk_advanced.ara_assessor to perform any object assessment.
- All delegates are considered licensed users and are tracked for their GRC usage.
- When the delegate logs in to perform the risk assessment on behalf of the assessor, the original assessor's name remains in the **Assessor** field. The new field **Assessor's delegates** displays the name of the delegate.
- The delegate can reassign the task to another user.
- The delegate can view the on-going assessments for the original assessor under **Tasks** in the Workspace.
- The delegate can create issues.
- The delegate can create risk response tasks and request approval.
- All activity performed by the delegate is captured in the activity stream.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Understanding the risk assessment instance

A risk assessment instance is where a risk assessor can assess risks and objects by responding to questions or factors.

After the risk assessment methodology (RAM) is created and the risk assessment scope is defined, the assessments are initiated by the risk administrator. The assessor receives a notification to assess the risks. To perform the risk assessment, an assessor must have the sn_grc.business_user role. The assessment is used to arrive at a risk score for an entity.

**Note:** You must manually assign the advanced risk assessment roles to the sn_grc.business_user role. To understand how you can adjust granting of roles and groups, refer to see the How to adjust granting of roles and groups to use background jobs [KB0963693] article in the Now Support Knowledge Base.

The questions that a risk assessor answers are configured in the RAM. An assessment can contain manual factors and automated factors. Manual factors need human input as responses. For automated factors, the responses are automatically calculated. Automated factors are automatically executed based on the schedule that is defined in their configuration.

After an assessment is completed, then based on the defined reassessment frequency, a reassessment is automatically triggered. A reassessment is triggered only if the existing risk assessment instance is in the Monitor state. If an assessment is in the Monitor state, then whenever automated factors run according to their schedule, the assessment scores will change and the factors will contribute new scores to the rollup.

If the risk assessor determines that an assessment must be reassigned to another relevant assessor, then the assessor can reassign the assessment. The assessor can also modify the responses after responding to the factors.

If an assessment is taken more than once, and if the option to copy the previous assessment responses is enabled in the RAM, then the responses from the previous assessments get automatically copied to the current assessment.

**Note:** Automated factor responses and overridden scores are not copied from previous assessments.

## Components of a risk assessment instance

Based on the configurations in the RAM, the risk assessment instance form also displays the following related lists:

- Previous Assessments: The previous five assessments for the risk that is currently being assessed.
- Risk Events: The number of risk events that are associated with the risk.
- Risk Indicators: The number of risk indicators that passed and failed for this risk.
- Open Issues: The number of open issues for the risk and their state and owners.
- Risk Response Tasks: The number of risk response tasks that are created for the assessment.
- Related controls: The controls that are related to the risk. This related list appears only when the control environment is being assessed.

  **Note:** Customers on previous releases might not be able to see the updated count for passed and failed indicators. To resolve this issue, run the *Update indicator and Controls Count* fix script.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

An assessor has the option to not assess the mitigating controls. The option to opt out of controls is useful in cases where there is a risk but there are no controls to mitigate it. For example, consider a scenario where a pandemic is a risk but there are no vaccines to control it. In such a case, the risk is assessed but the controls can be left out of the assessment. When an assessor decides to opt out of assessing mitigating controls and residual risks, the score is set to **Not applicable**.

If the control assessment is configured to assess individual controls, and the controls are associated with the risk being assessed, then the option to opt out of controls does not appear. This happens because the controls are defaulted.

If the residual assessment is for inherent risks and controls, and if the risk assessor opts out of control assessment, then the residual risks are not applicable. This condition is created because if there are no controls, that automatically means there are only inherent risks and no residual risks.

## Stages of risk assessment

The risk assessment life cycle goes through the following states:

1. Ready to assess: A new assessment instance is created.
2. Inherent assessment: The inherent risk assessment is performed.
3. Control assessment: The control assessment is performed.
4. Residual assessment: The residual risk assessment is performed.
5. Target assessment: The target risk assessment is performed.
6. Respond: You respond to the risks.
7. Awaiting approval: The risk assessment is awaiting approval from the approvers if they have been identified.
8. Monitor: The risk assessment is complete and is being monitored.

### Managing risk responses

A risk response is the strategy used to deal with risks after the risks are assessed.

After risks are assessed, the assessor determines how to approach those risks. To deal with the risks, the assessor can choose from the following types of risk responses or strategies:

- Accept: Accept the risk as it is.
- Mitigate: Identify and implement additional controls to mitigate the risk.
- Avoid: Change the plan to completely avoid the risk.
- Transfer: Transfer or share the risk with a third party.

After an assessor identifies the best strategy, the assessor then creates risk response tasks and assigns them to the risk user with the role sn_risk.user. Each strategy is explained as follows:

Risk acceptance

When risk users accept a risk, they provide a plan for how they want to accept the risk, provide a justification for accepting the risk, and seek additional approval from the risk owner. Closure of the acceptance task implies you are accepting this risk for that time period. The risk then moves to the Monitor state. After the specified time period is over, you can re-initiate the workflow to assess the risk and then you can again respond to the risk. The risk owner can then respond with one of the following options:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Approve
- Reject
- Cancel
- Request more information
- Decide that it is no longer required

Risk mitigation

When risk users choose to mitigate a risk, a risk mitigation task is created. The risk user must provide a plan for how to mitigate the risk and request a review from the risk manager. When the risk mitigation task is in the Draft or Work In Progress state, you can either create more risk-mitigating controls for the risk or add existing controls from the library. The reviewer with the role sn_risk.manager then reviews the plan and selects one of the following options:

- Close
- Revert to draft state and provide additional comments
- Cancel
- Delete

Risk avoidance

When risk users choose to avoid a risk, they provide a plan for how they want to avoid the risk and request a review from the risk manager. The reviewer then reviews the plan and can select one of the following options:

- Close
- Revert to Draft state and provide additional comments
- Cancel
- Delete

Risk transfer

When risk users choose to transfer a risk, they provide a plan for how they want to transfer the risk and request a review from the risk manager. The reviewer then reviews the plan and can select one of the following options:

- Close
- Revert to Draft state and provide additional comments
- Cancel
- Delete

**Note:** The risk response workflow is not available for an object assessment.

### Risk score rollup in Advanced Risk Assessment

In Advanced Risk Assessment, risk scores are calculated across risk statement hierarchy, entity hierarchy, or a combination of both. These methods enable stakeholders to monitor their risk posture and provide visibility of the overall aggregated risk score.

Before you understand the rollup feature, consider the following points:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Each entity might have multiple scores based on the different risk assessment methodologies.
- Only the risk assessments in the **Monitor** state contribute to the risk score.
- Each risk assessment methodology might have a different formula to calculate the rollup qualitative score and the rollup quantitative score. The formula is specified in the **Rollup configurations**section in the risk assessment methodology form.
- Whenever the Advanced Risk plugin is activated the risk scores get rolled up.

### Risk statement hierarchy

Based on the assessments, the system automatically rolls up the inherent risk scores, the Annual Loss Expectancy (ALE), control effectiveness score, residual risk score, and ALE across the risk statement hierarchy for the selected methodology. This rollup allows the risk managers to monitor their enterprise risk posture.

### Entity hierarchy

Like risk statement hierarchy, the system also automatically rolls up the risk scores and ALE values across the entity hierarchy for a risk assessment methodology. This rollup allows the entity owner to monitor the entity's risk posture. The rollups are done using the following formulae:

- Sum
- Average
- Maximum
- Minimum

### Entity hierarchy and risk statement

Using the Manage Aggregated Risk report, customers can define additional reporting dimensions on which they want to monitor the risk posture for an entity. For example, if you want to understand an internal fraud related risk for Retail Banking, you can define that reporting dimension and monitor the risk.

### Changes in reports and risk rollup method after migrating to Advanced Risk Assessment

To utilize the new rollup score calculation, the risk administrator, with the role sn_risk.admin, must first enable the *Migrate to Advanced Risk Assessments* property by navigating to **Advanced Risk Assessment** > **Administration** > **Properties**. This property is not enabled by default.

**Note:** It is crucial to note that when you enable the mentioned property, any customizations in the risk overview dashboard will be hidden. Contact ServiceNow for assistance. Also, the following properties in risk are not hidden when you migrate to advanced risk rollup:

- Compare risk tolerance based on
- Compare calculated risk score with

When customers migrate to Advanced Risk, the following reports are hidden from the user's view:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Aggregated Risk Report
- Exposure by Entity
- Exposure by Risk Statement

In the Risk Overview dashboard, the following tabs are hidden:

- Entity Tolerance Status
- Risk Tolerance Status
- Aggregated Entity Information
- Aggregated Risk Information

Under the Aggregated Risk Report, the following modules are visible that show the rolled up risk scores:

- Aggregation by Risk Statements
- Aggregation by Entities
- Entity by Risk Statements

When you migrate to advanced risk assessment, individual risk score values do not roll up to give you the risk score. Instead, the values from advanced risk assessment are considered. For example, for an entity, in the Entity form, the Risk Rollup and Tolerance section is not displayed. The same applies to any risk statement. Instead, a related list called Aggregated Risk is displayed. The Aggregated Risk related list contains the following values derived from various risk assessments:

- Risk assessment methodology
- Residual rating
- Inherent rating
- Control effectiveness
- Residual ALE
- Inherent ALE
- Contributing risk assessments
- Risk rollup status

### Privacy risk management

As users of Privacy Management, you can perform advanced risk assessments with a limited set of features even if you do not have the complete license for Integrated Risk Management.

To prioritize the areas that need attention, risk assessment is performed by various stakeholders and is embedded as part of different workflows in an organization. For example, within Privacy Management, users must be able to identify the assets that pose the highest risks and ensure appropriate levels of controls are implemented to mitigate those risks. To address this need of risk assessment in other business units, a solution is implemented to enable the users of Privacy Management to use the advanced risk assessment capability, with limited features, without buying the Integrated Risk Management license for their risk management needs.

The following are the key points to consider when users use the limited advanced risk assessment for their risk assessments.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

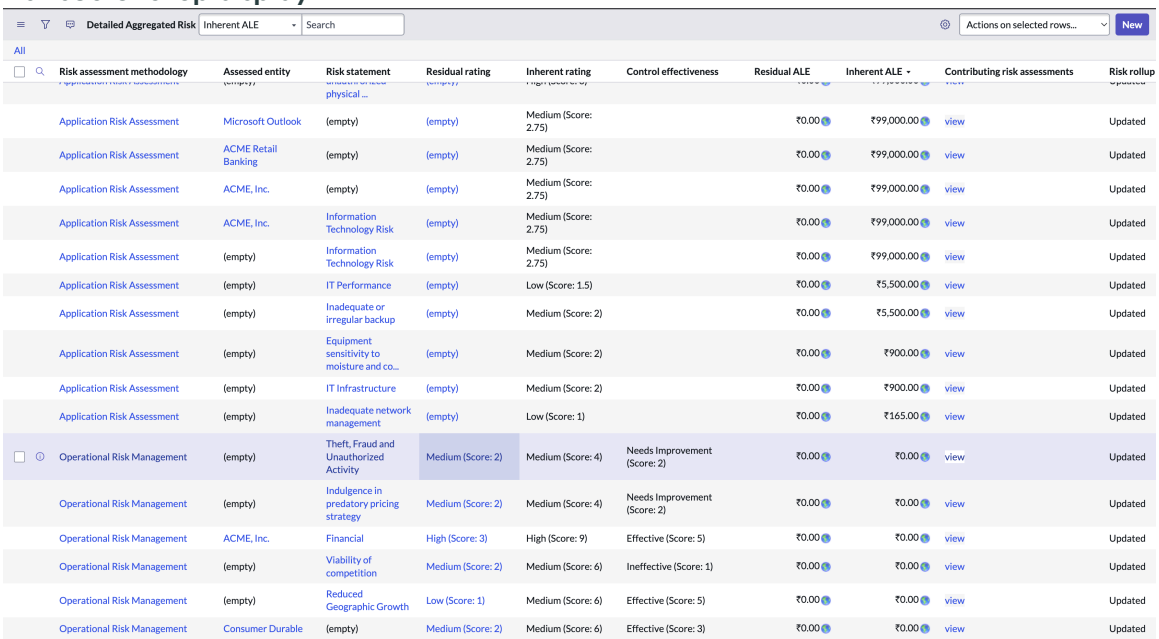
- The lite users of other business units can only have two published risk assessment methodologies.
- Automated factors are available for use.
- Managing risk events and using the risk identification workflow are not available in limited risk assessments.

### Risk score rollup in Privacy Management

When users of Privacy Management perform advanced risk assessments, they get the risk scores automatically rolled up.

Starting with version 14.0, users of Privacy Management can perform advanced risk assessments. Risk scores are rolled up when you perform advanced risk assessments. Rolled up scores show the aggregated risk results. The rolled up aggregated scores are displayed on the tables as shown in the following figure.

**Risk score rollup display**




| Risk assessment methodology | Assessed entity | Risk statement | Residual rating | Inherent rating | Control effectiveness | Residual ALE | Inherent ALE | Contributing risk assessments | Risk rollup |
|---|---|---|---|---|---|---|---|---|---|
| Application Risk Assessment | Microsoft Outlook | (empty) | (empty) | Medium (Score: 2.75) | | ₹0.00 | ₹99,000.00 | view | Updated |
| Application Risk Assessment | ACME Retail Banking | (empty) | (empty) | Medium (Score: 2.75) | | ₹0.00 | ₹99,000.00 | view | Updated |
| Application Risk Assessment | ACME, Inc. | (empty) | (empty) | Medium (Score: 2.75) | | ₹0.00 | ₹99,000.00 | view | Updated |
| Application Risk Assessment | ACME, Inc. | Information Technology Risk | (empty) | Medium (Score: 2.75) | | ₹0.00 | ₹99,000.00 | view | Updated |
| Application Risk Assessment | (empty) | Information Technology Risk | (empty) | Medium (Score: 2.75) | | ₹0.00 | ₹99,000.00 | view | Updated |
| Application Risk Assessment | (empty) | IT Performance | (empty) | Low (Score: 1.5) | | ₹0.00 | ₹5,500.00 | view | Updated |
| Application Risk Assessment | (empty) | Inadequate or irregular backup | (empty) | Medium (Score: 2) | | ₹0.00 | ₹5,500.00 | view | Updated |
| Application Risk Assessment | (empty) | Equipment sensitivity to moisture and co... | (empty) | Medium (Score: 2) | | ₹0.00 | ₹900.00 | view | Updated |
| Application Risk Assessment | (empty) | IT Infrastructure | (empty) | Medium (Score: 2) | | ₹0.00 | ₹900.00 | view | Updated |
| Application Risk Assessment | (empty) | Inadequate network management | (empty) | Low (Score: 1) | | ₹0.00 | ₹165.00 | view | Updated |
| Operational Risk Management | (empty) | Theft, Fraud and Unauthorized Activity | Medium (Score: 2) | Medium (Score: 4) | Needs Improvement (Score: 2) | ₹0.00 | ₹0.00 | view | Updated |
| Operational Risk Management | (empty) | Indulgence in predatory pricing strategy | Medium (Score: 2) | Medium (Score: 4) | Needs Improvement (Score: 2) | ₹0.00 | ₹0.00 | view | Updated |
| Operational Risk Management | ACME, Inc. | Financial | High (Score: 3) | High (Score: 9) | Effective (Score: 5) | ₹0.00 | ₹0.00 | view | Updated |
| Operational Risk Management | (empty) | Viability of competition | Medium (Score: 2) | Medium (Score: 6) | Ineffective (Score: 1) | ₹0.00 | ₹0.00 | view | Updated |
| Operational Risk Management | (empty) | Reduced Geographic Growth | Low (Score: 1) | Medium (Score: 6) | Effective (Score: 5) | ₹0.00 | ₹0.00 | view | Updated |
| Operational Risk Management | Consumer Durable | (empty) | Medium (Score: 2) | Medium (Score: 6) | Effective (Score: 3) | ₹0.00 | ₹0.00 | view | Updated |

For more information to understand the rollup of scores, see Risk score rollup in Advanced Risk Assessment.

### Manage risk assessment scheduler

Create a risk assessment scheduler and assign it to the risk manager. A risk manager can then identify the entities and the risks within the entities for bulk initiation of risk assessments.

In most organizations, the second line of risk managers coordinates the risk assessments. This second line of risk managers identifies the entities and the risks within those entities for risk assessment. They also identify who must assess the identified risks. This process is like a risk assessment campaign the risk managers must manage until the first line of risk managers reach the level of maturity where this is no longer required and the first line of risk managers can self-assess and report these risks. Because of this cycle of risk assessment, the risk managers are expected to create individual risk assessment scopes and initiate risk assessments. This repetitive activity results in loss of time for risk managers. To address this issue, a new form called Risk Assessment Scheduler has been introduced in the Quebec release. The risk assessment scheduler enables the risk manager to select the:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Risk assessment methodology
- Entities that must be assessed
- Assessors of the assessment
- Frequency with which the risks must be reassessed.

Based on this information, the system automatically creates the risk assessment scope and initiates the risk assessments for those entities at the defined frequency. All the risks that are mapped to the entity are considered to be in scope for assessment.

The following figure shows the states, the descriptions, and the expected outcomes of each of the actions for the risk scheduler form:

**Workflow and actions of the risk assessment scheduler**

| State | New | Scope Definition | Complete |
|---|---|---|---|
| **Description** | This is the state of the record when a new risk scheduler record is created. | This is the state when the risk manager defines the scope of the risk assessments which includes the entities, when they should be assessed, and who should assess it. | This is the state when the system bulk initiates the risk assessments for the selected entities to the respective assessors. |
| **Expected Outcome** | The user selects the risk assessment methodology for which they need to bulk initiate assessments. | The user selects the entities that must be assessed, the assessor who should assess these risks, and the frequency of reassessment, if applicable. | The system automatically creates the risk assessment scopes for those entities and bulk initiates risk assessment tasks for the respective risks in those entities. |
| **Available Actions** | **Define assessment scope –** This is the only action that the user can take in this state. Once this action is taken, the record moves into scope definition state. The entities selected in the next state are filtered based on the risk assessment methodology selected | **Add –** Using this action, the risk manager can add entities that must perform the risk assessment. The list is filtered based on risk assessment methodology.<br><br>**Change methodology –** This action takes the record back into the new state where the user can change the risk assessment methodology, if required.<br><br>**Finalize –** After the entities are selected, the assessors are defined. The user can use this action to initiate the risk assessments. | |

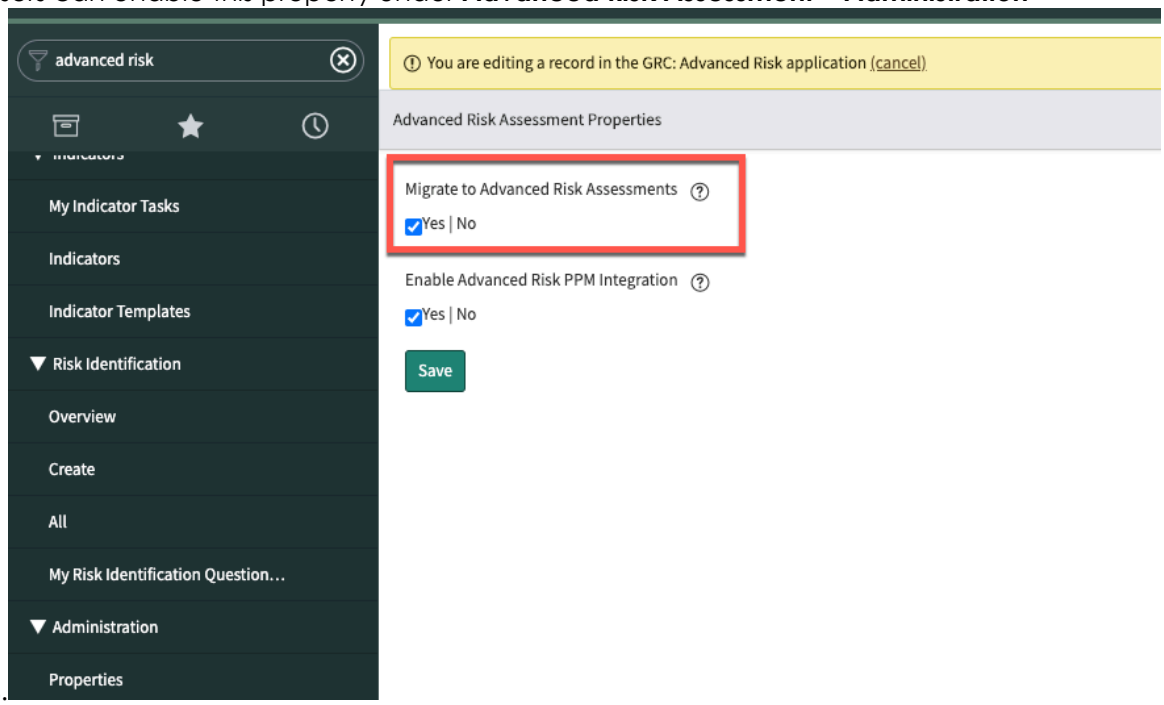
### Integration of advanced risk assessments with risks and controls

When customers migrate to advanced risk assessments, the system replaces the legacy risk life cycle and shows a new section called Assessment Summary on the Risk form. This section is useful for the risk managers as it provides the overall visibility of the assessment results.

Migrating to advanced risk assessments is useful for the risk managers as they can view the risks that need immediate attention. To migrate to advanced risk assessment, a new property called *Migrate to Advanced Risk Assessments* is introduced in the Quebec

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

release. Users can enable this property under **Advanced Risk Assessment** > **Administration** > **Properties**.

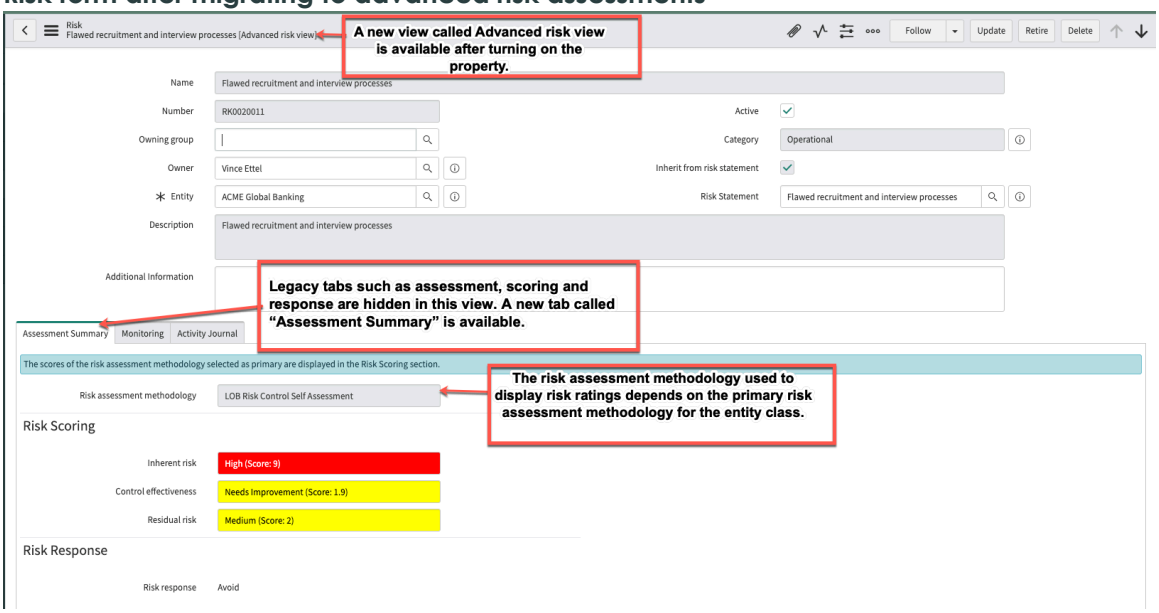



When users enable this property, they completely migrate to the advanced risk assessment and do not use the old risk management. This migration affects the following forms:

- Risk
- Entity
- Risk Statement

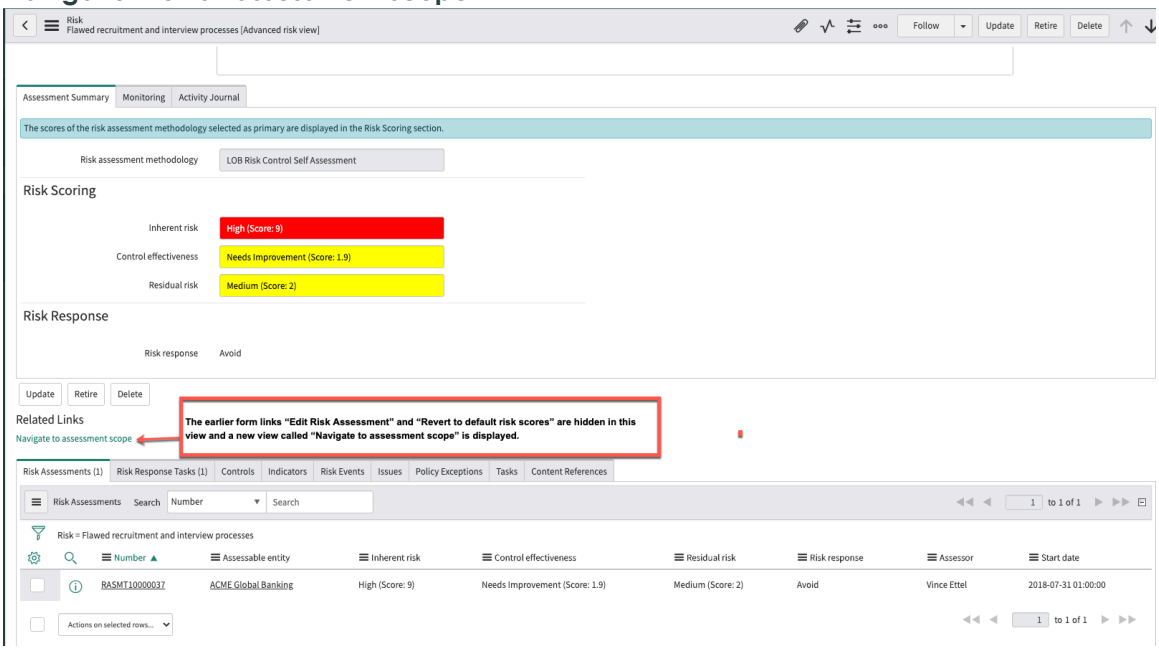
When users migrate, the system then removes the legacy risk life cycle, scoring, assessment, and response sections on the risk form. Instead, a new section called Assessment Summary is available where the risk assessment scores are displayed along with the risk response. If there are multiple methodologies used for risk assessment, the system detects the default methodology for the selected entity class and displays those scores in this field. The primary risk assessment methodology can be defined in the risk assessment methodology form.

### Risk form after migrating to advanced risk assessments




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Navigation to risk assessment scope




Similarly, for controls, the control effectiveness values are updated if individual assessment of controls is performed.

On the Entity form, the aggregated risk scores are displayed from the primary risk assessment methodology. The old tabs displaying the legacy risk scores are hidden from the user's view.

On the risk statement form, fields like assessment, framework, and scoring are hidden. The corresponding old links for pushing risk scores and so on are also hidden from the user's view.

### Risk appetite and tolerance in Advanced Risk

You can define a risk appetite and tolerance within your organization by using the Advanced Risk application. A risk appetite and tolerance enable your organization to define the boundaries for acceptable and unacceptable risks.

## Overview of a risk appetite

A risk appetite is the amount of risk that an organization is willing to take to achieve its strategic objectives.

A risk appetite can be defined in qualitative (numerical scale and ratings) and quantitative (absolute dollar) terms. For example, let's say that a lending institution provides a loan to some small scale industries. The lending institution has defined 5 percent as their target non-performing asset (NPA) for the current fiscal year.

**Note:** A non-performing asset (NPA) is a loan or advance for which the principal or interest payment remained overdue.

Therefore, the risk appetite of the institution is 5 percent.

## Benefits of using a risk appetite

The benefits of having a risk appetite for your organization are as follows:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Provide better guidance to your first line of employees to implement risk management in specific areas of your business.
- Take risks within your organizational expectations and define and manage actions when there's a breach.
- Assess the risk status that is based on the defined risk appetite and prioritize the risks that require attention.
- Assess all possible risks and define the boundaries for acceptable and unacceptable risks.
- Monitor your risk exposure and ensure that it's consistent with your risk appetite. You can also track any unacceptable risks.
- Initiate a risk mitigation plan based on the risk appetite status.

## Overview of risk tolerances

A risk tolerance is the standard deviation from the defined risk appetite that an organization can withstand without risking the organization's objectives and goals.

## Setting up a risk appetite and tolerance

A risk administrator can configure and set up a risk appetite for your organization in the Advanced Risk application. For more information, see Risk appetite setup.

### Target risk assessment in Advanced Risk

You can perform a target risk assessment to define your desired future risk level using the Advanced Risk application. The target risk assessment enables you to assess your target risk posture and monitor progress toward its achievement.

## Overview of a target risk assessment

A target risk assessment is an assessment type to define the desired risk level the organization want to achieve in the future. By evaluating the desired level of likelihood and impact of identified risks, organizations can establish target risk levels for each risk.

For example, when assessing a risk, organizations consider various aspects such as inherent risk, the effectiveness of controls, and residual risks. However, it's equally important to capture the desired risk level that will be attained after the risk response is implemented. The target risk represents the optimum level of risk that you aim to achieve after your action plan is successfully executed. It enables you to measure the benefits your organization gets in relation to the cost of implementing those actions.

## Setting up a target assessment

A risk administrator can configure and set up a target risk assessment for your organization in the Advanced Risk application. Risk administrator can enable the option for assessing a target risk on the Risk assessment methodology (RAM) form. For more information, see Configure a target assessment.

**Important:** You can enable target risk assessment for existing published RAMs. However, after you enabled, it can't be turned off. Additionally, target risk assessment can only be conducted for new assessments and not for assessments that are already in progress.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Assessing a target risk

Assessors can analyze the future state of the risk based on the defined factors, scoring logic, and rating criteria in the RAM form. Assessing the future state of risk is a structured process that shares similarities with inherent, control, and residual assessment types. Based on the target risk profile, the system also computes the future risk appetite status. It enables assessors to analyze if the target risk profile is in line with the risk appetite or not. Risk approvers can review the target risk rating and the future appetite status and approve them. Target risk assessment can be performed for both risk and object-based assessments. However, if it's object-based, the future appetite status isn't computed and displayed. For more information, see Perform advanced risk assessment in the Risk Workspace.

**Important:** If target risk assessment is enabled for a methodology, the risk or object can only be assessed in the next experience.

## Reporting a target risk

On the heatmap, you can view the target risk profile, which provides a comprehensive understanding of the inherent, residual, and target states of the risk. When the risk assessment criteria are shared, you can analyze the risk movement from inherent state to residual state and then to its target state. By using the risk trend capability, you can assess risk changes over the past five periods to determine if it's moving in the desired direction. For more information, see Risk heatmap workbench.

## Manage risk events

Risk events are potential or actual financial and non-financial losses, near misses, and gains that occur within an organization. Risk events are also known as loss events or loss entries.

To effectively manage risks, it's essential to monitor risk events. You must relate them to existing risks, perform a root-cause analysis, and track the remedial tasks. Organizations use risk events to understand their losses and to manage their risks more efficiently. Risk events do not only lead to losses. At times, risk events also result in gains for an organization. For example, in the banking industry, if there's an error in a trading algorithm, it might result in a gain for an organization.

Any employee can report a risk event. After a risk event is reported, it is analyzed by the risk manager.

Risk events can be of two types:

Internal risk events

: Events that occur within your organization.

External risk events

: Events that occur in other organizations but are shared with the industry to ensure that other organizations can prevent them.

You can create a risk event using either the Service Portal or your ServiceNow instance. Risk events provide the following:

- Concrete data that enables you to better quantify and validate existing risks.
- Visibility into new risks because risk events often recur.

You can view the risk events dashboards by navigating to **Risk Events** > **Overview**.

For information on how to configure risk event integration in the Risk Workspace, see the Risk event integration in workspace [KB0966898] article in the Now Support Knowledge Base.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

Risk events life cycle

### Risk events life cycle

After a risk event is created, the event goes through a life cycle where risk managers analyze it and send it for approval.

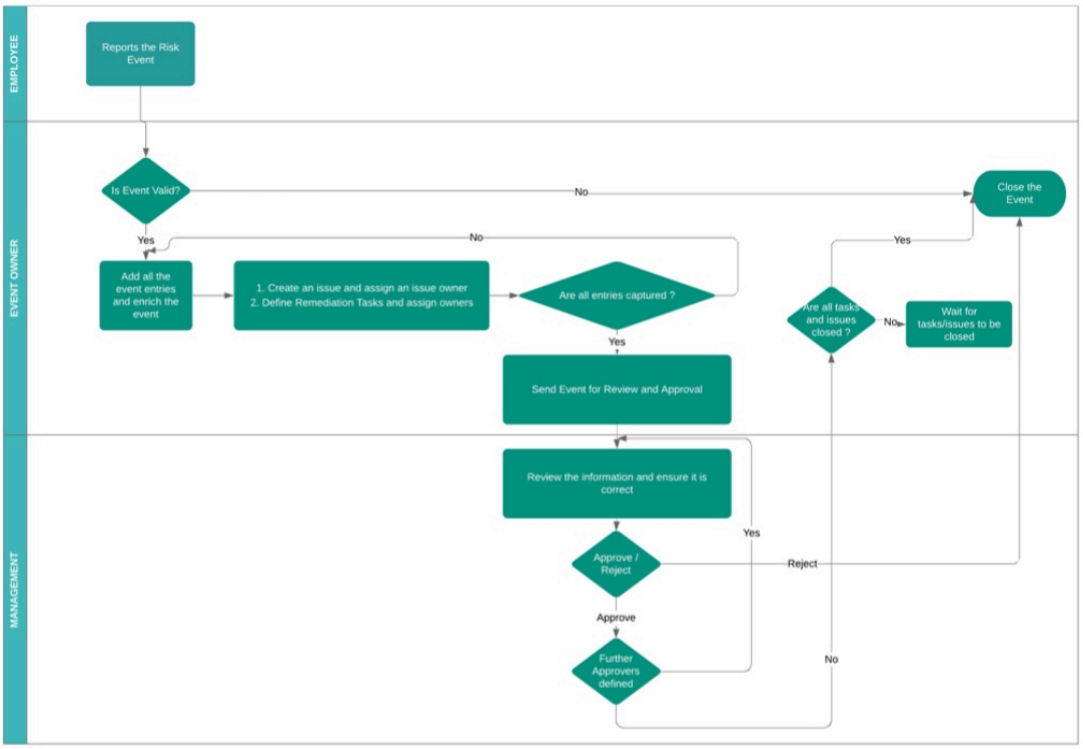
The life cycle for risk events goes through the following stages:

1. Creating a risk event: A new event is reported by a business user. The event is pending validation by the event owner or risk manager who has the sn_risk.manager role.
2. Analyzing the risk event: The risk manager analyses if the event is legitimate and adds all the important information such as the event's loss entries, approvers, the root cause of the event, and the preventative and remedial action for the event. In this state, additional information can be requested from the event creator. You can then create an issue to ensure that similar events do not occur in the future. The issues are assigned to the respective issue owners who can then either accept the issue as is or create a remediation task.
3. Awaiting approval for the risk event: After all the data is entered and validated, the risk manager may request that the event be approved. The need for approval is determined by the loss threshold defined by the organization. For example, your organization may decide that if a risk event leads to a loss of $100000, then it must be approved by the senior risk management teams. Each event might go through several rounds of approval.
4. Approving, rejecting, or canceling a risk event: After the event is approved, the risk manager ensures that the issues created for the risk event are closed and that the root-cause analysis (RCA) is complete before the event is closed. At this stage, the approver can also choose to reject or cancel the event with adequate reasons.
5. Closing a risk event: After a user with the sn_risk.manager role is certain that the event has been captured and that the RCA has been completed, the event coordinator can close the risk event. If a risk event has open issues and tasks, then the risk event cannot be closed until the associated issues and tasks are closed.

The risk events workflow is summarized in the following figure:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Risk events workflow




Related topics

Create a risk event in the Risk Workspace

#### Relationship between risks, risk events, and risk statements

Relating risk events to risks and relating a risk statement to a risk is important for all organizations that use the Risk Management application. Properties to enable these relationships are provided under *Risk Event Properties* and Risk Management properties.

## Relationship of risk events to risk

Consider relating risk events to risks if you use the Risk Management application. This relationship provides data for future risk assessment and is also useful for accurate reporting. For example, if the management of an organization wants to know the total loss incurred due to internal fraud, it can only be reported if all the risks are related to the internal fraud risk event. To relate risks events to risk, set the *Make risk event to risk relationship mandatory* property to Yes. By default, this property is not turned on.

## Relationship of risk statement to risk

Consider relating each risk statement to a risk. Establishing this relationship prevents the creation of orphan risks. An orphan risk is a risk that does not have a corresponding risk statement associated with it. For example, if all the business units within an organization understand the risk of employee attrition in different terms, it is difficult for the organization to maintain comprehensive data on the risk of attrition. It is easier if the risk statement of Employee Attrition is attributed to all events that relate to this risk. Establishing the relationship between a risk statement and a risk is vital for correct reporting and prevention. To relate risks to risk statements, set *sn_risk.risk_statement_mandatory* to True.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Add Basel categories to risk statements

The Basel categorization is specific to the banking industry. This categorization helps customers comply with the Basel regulations by automating their loss event reporting. This particular setting enables the users to view the Basel Dashboards. The Basel Dashboard shows the number of loss events and net loss based on the Basel business lines and categories. Enabling this setting enables the users to view the Basel categorization tab where users can select one of the following Basel categories that apply.

- Internal fraud
- External fraud
- Employment practices and workplace safety
- Clients, products, and business practice
- Damage to physical assets
- Business disruption and system failures
- Execution, delivery, and process management

For more information, see Properties installed with Advanced Risk and Properties installed with Risk Management

To enable Basel categorization, set *Show Basel attributes and reports* to **Yes**.

### Risk event response template

The risk event response template automates the process of adding approvers, issues, and owners to a risk event. This automation is based on the conditions defined in the template.

The risk event response template provides these primary benefits:

- reduces the need for human handling of risk events during risk event creation.
- automatically defines the risk event life cycle and how users respond to that risk event.
- saves time with a predefined template.

For example, consider that a health and safety risk event has occurred. If the template is defined, the template can be used to assign the event to the person responsible for health and safety. The template facilitates the automatic assignment of risk events by enabling you to choose event types, entities, categories, and so on.

Users can define the threshold amount for risk event approvers. The threshold is defined based on the risk appetite of the customers. For example, an organization decides that a risk event resulting in a loss of $1000, does not need an approver. This threshold of $1000 can be defined in the template. If the organization determines that any amount greater than $1000 dollars needs approval, the template can automatically assign an approver.

You can define the template for any entity. All the child entities of the parent entity inherit the rules defined in the risk event response templates. Defining a template saves the time and effort required to define the rules for each entity separately.

For more information on how to set up risk event ingestion, see KB0780985 article in the Now Support Knowledge Base.

### Associate similar risk events

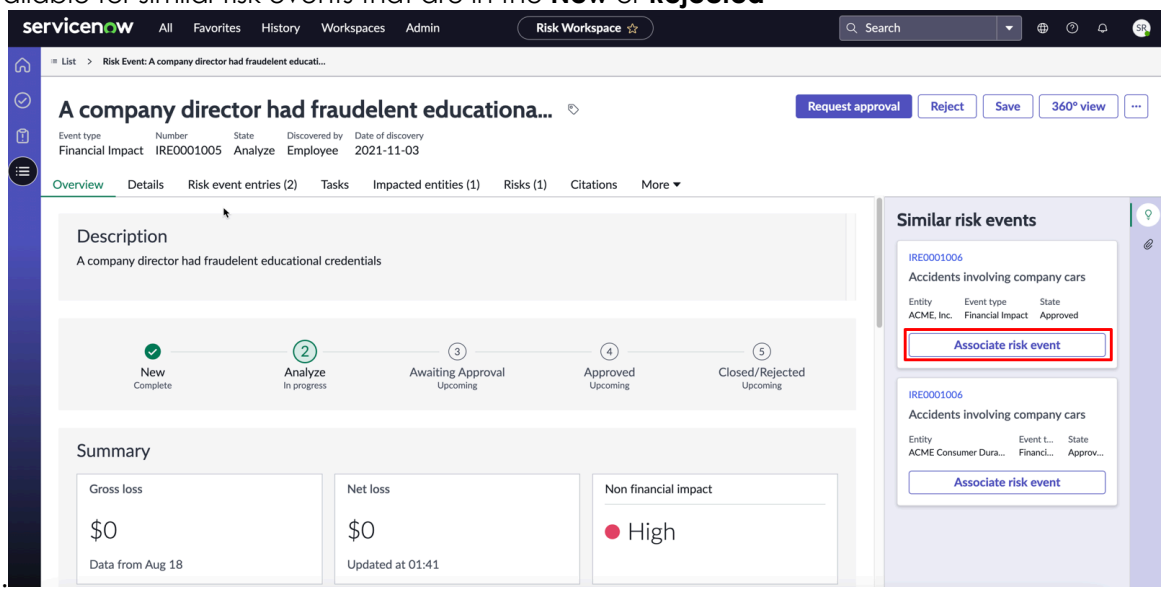
Train a similarity solution definition that uses machine learning by activating the Governance, Risk, and Compliance: Predictive Intelligence plugin. The solution enables the system to display similar risk events automatically.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Governance, Risk, and Compliance: Predictive Intelligence plugin uses Artificial Intelligence (AI) and Machine Learning (ML) to manage the risk events more efficiently. You can identify similar risk events and group them to capture and analyze the actual impact of the risk event.

For example, in an organization with operations in multiple locations, the risk event teams across different locations may be working on similar types of risk events. This challenge results in duplicate efforts to manage the risk events within the organization. This capability reduces the manual effort in managing similar risk events and improves overall organizational efficiency.

You can associate similar risk events only when the main risk event is in the **Analyze** state. Also, the Associate risk event button is unavailable for similar risk events that are in the **New** or **Rejected** state.




The platform machine learning administrator (ml_admin) can create a solution definition and modify an existing one. You can navigate to **Risk Events** > **Administration** > **Properties** to update the risk event property with the new solution definition name.

## Business process management

A business process is an activity or a set of activities that can accomplish a specific organizational goal.

A business process is anything that happens within your organization and that has a well-defined start and finish. Examples of business processes in the banking industry are the customer onboarding process and the credit check process. Because each business process is unique, they may have different levels of criticality and impact. Business processes must be managed with a comprehensive life cycle. They may also have different risks and different controls that must be identified. With the Quebec release, the creation of a business process is enhanced. As an enterprise architect or a service owner, you can do the following:

- Define a new business process.
- Manage the life cycle of the process.
- Define the owners of the process.
- Define the relationship of the new process to a specific process, such as if the new process is a parent process or a child process.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Define the business impact and the criticality of the process.
- Review the process periodically for improving efficiency.

### Life cycle of a business process

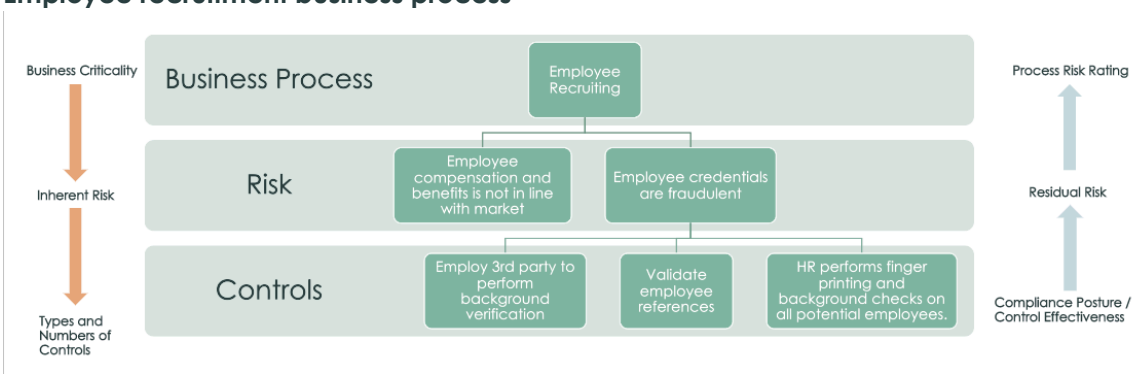
The life cycle states of a business process are as follows:

1. **Draft**: This state is the default state when a business process is created and its relationship to various risks and controls is defined. If no reviewers are selected to review the process, then the process is directly published.
2. **Review**: If reviewers are selected, the process is sent to the reviewers before it is published.
3. **Published**: After the review is complete, the process is published.
4. **Retired**: The process is no longer required.

**Note:** Even when a process is Retired, it stays in the system for audit purposes.

The following image shows an example of how to define a business process, such as employee recruitment. You can define the relationship of the process with the associated risks and controls. You can also determine how associating the risks and controls helps to derive the risk rating of the process.

**Employee recruitment business process**




Related topics

Create a business process

## Manage risks, risk statements, and risk frameworks

The risk library contains all risk frameworks and risk statements. Risk frameworks are used to group risk statements into manageable categories, while risk statements group the individual risks. The risk register is the central repository for all potential risks that could occur at any time, anywhere in the organization.

### Assess risks and develop risk statements

Assessing risk means identifying and analyzing the threats and vulnerabilities that could adversely affect your organization's business objectives. Risk is a function of the likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. By identifying your risks and the impact and likelihood of those risks occurring, your organization can prioritize control testing and remediation activities. It also helps you understand the true business impact when a control fails.

A good risk statement should answer:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- What could happen?
- How could it happen?
- Why do we care?

### Workflow of a risk using Advanced Risk

When you migrate to advanced risk assessment, you can view the various states of the risks take the necessary actions. This ability simplifies your view of the risk form.

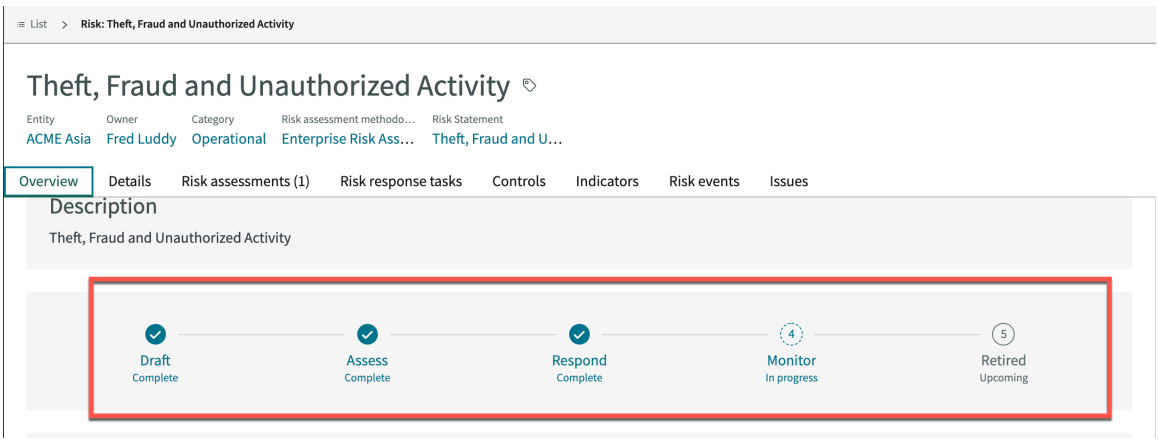
When your risk administrator enables the *Migrate to Advanced Risk Assessments* property located under **Advanced Risk Assessment** > **Administration** > **Properties**, the life cycle of the classic or legacy risks undergo a change. You can also initiate a risk assessment directly from the risk form.

**Note:** Once you enable this property, you cannot disable it.

Prior to version 14.0, when the *Migrate to Advanced Risk Assessments* property was enabled, the risks were only classified as either active or inactive. Starting with version 14.0, as a risk owner, when you enable Advanced Risk, you can view the following states of your risks.

1. Draft
2. Assess
3. Respond
4. Monitor
5. Retired

**States of a risk with advanced risk assessment**




All the states and the actions available for each state are explained in the following table.

| State | Description | Actions available |
|---|---|---|
| Draft | This is the state of a risk when a risk is created by the second line of defense or identified by the first line of defense.<br><br>The objective in this state is to map and identify the risk pertaining to your | • **Save**<br>• **Assess**: Pushes the workflow and initiates the risk assessment.<br>• **Monitor**: If you do not want to assess the risk but want to monitor the risk. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| State | Description | Actions available |
|---|---|---|
| | organization. If you modify the entity or the primary risk assessment methodology (RAM) for a risk, the state of the risk gets updated based on the primary RAM's latest assessment. | • **Retire**: The risk is retired along with all underlying risk assessment and risk response.<br>• **Navigate to assessment scope**: Shortcut to risk assessment scope. The primary risk assessment methodology is passed.<br>• **360 degree**: View the complete 360-degree relationships for the risk. |
| Assess | This is the state of a risk when advanced risk assessment is initiated and being performed. If there is a response strategy, then the risk moves to the Respond state otherwise it moves to the Monitor state once the assessment is completed. | • **Save**<br>• **View assessment**: Navigates to the actual risk assessment form.<br>• **Cancel assessment**: If you want to cancel the current assessment. The respective risk assessor is notified about the canceled assessment.<br>• **Return to draft**: Cancels the current assessments and returns the risk to the previous state.<br>• **Retire**<br>• **Navigate to assessment scope**<br>• **360 degree** |
| Respond | This is the state of the risk when the risk response task is in progress.<br><br>Once the risk response task is closed, the risk is automatically moved into the Monitor state | • **Save**<br>• **Assess**: Pushes the workflow back in the workflow. The in-progress risk response task would be canceled.<br>• **Retire**<br>• **Navigate to assessment scope**<br>• **360 degree**<br>• **Return to draft** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| State | Description | Actions available |
|---|---|---|
| Monitor | This is the state of the risk when the risk has been assessed and the response task is closed.<br><br>If KRIs are defined (through Metrics), they are executed to monitor the risk. | • **Save**<br>• **Assess**: Moves the risk back to Assess state and initiates the risk assessment.<br>• **Retire**<br>• **Navigate to assessment scope**<br>• **360 degree**<br>• **Return to draft** |
| Retire | This is the state of the risk when the risk is no longer valid but the organization wants to keep a system of record for audit purposes. | • **360 degree**<br>• **Activate**: Reactivates the risk and moves it back to Draft state.<br>• **Navigate to assessment scope**. |

### Manage risks linked to the same risk statement

You can create and associate multiple risks to the same risk statement and entity combination. This association benefits the risk managers and the entity owners.

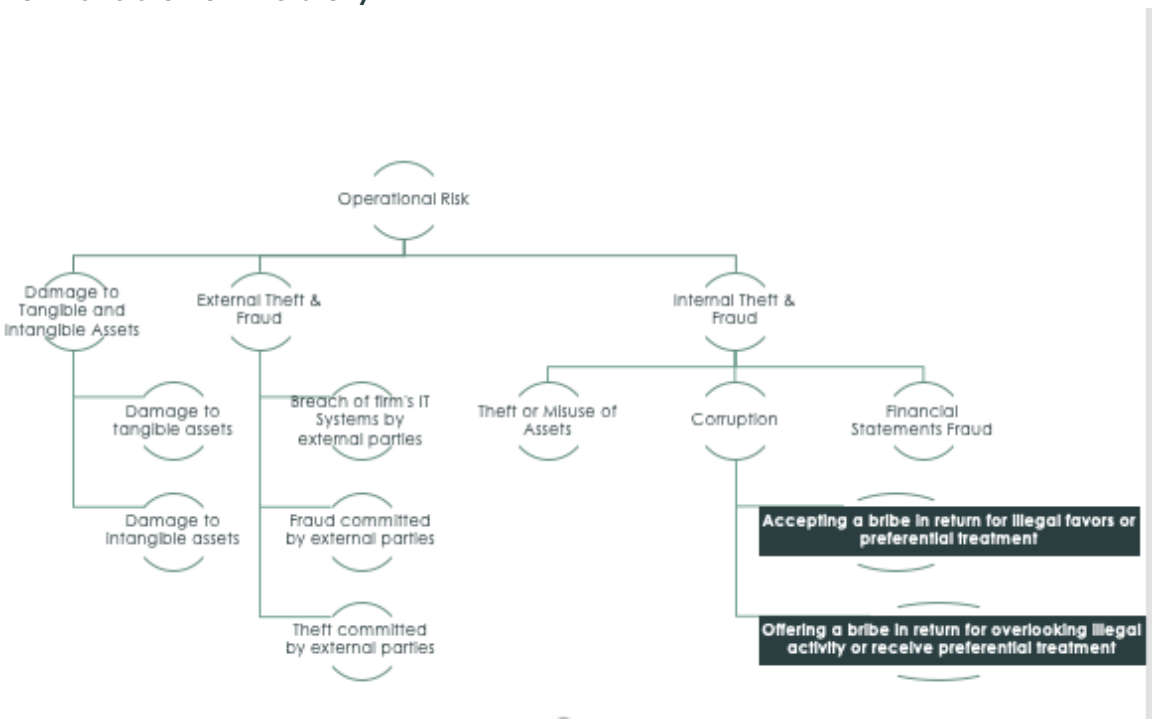
Before the latest release, users could only associate one risk for a single entity and risk statement combination. This ability was useful for customers who have a mature risk program with a well-defined and standardized risk taxonomy. However, it did not meet the requirements of customers who do not have a standardized risk taxonomy. Such customers usually have only two or three levels of risk statement hierarchy while their actual risks are still local for each business unit or lines of business. Also, when the first line identifies new risks, they associate those risks to an enterprise risk hierarchy. This allows the new risk scores to aggregate and impact the overall risk hierarchy. With the current release, a new option called **Inherit from risk statement** is introduced on the Risk form. If this option is selected, the risk creation happens in the previous manner. This means that there can be only one instance of risk statement and entity combination. However, if this option is not selected, the system allows the risk statement hierarchy to be used as categorization and sub-categorization hierarchy and associates multiple risks to the same risk statement and entity combination. This option also enables the first line to associate their newly identified risks to the risk hierarchy at a level they want to. When this new option is not selected, the system assumes that the name and description of the risk is overridden and must not be the same as the risk statement name and description.

This feature benefits the risk manager as it allows the risk managers to define the risk taxonomy according to the needs of their organization. It also benefits the entity owners to identify risks for their entity and link them to enterprise risk taxonomy.

To understand this feature, see the following image and consider the example. Most customers have risk statements defined until Corruption. Anything lower than Corruption such as accepting a bribe is defined as a risk as it is difficult to harmonize these risks across the organization. This feature of linking multiple risks to the same risk statement and entity enables customers to prevent the creation of orphan risks with no one acting on them.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### New risk statement hierarchy




### Risk hierarchy and scoring

Starting with New York, risk managers can create hierarchies that include different types of risk (operational risk, IT risk, or strategic risk). Once the underlying risks are assessed, the risk scores are automatically rolled up across the risk statement hierarchy, providing better tactical and strategic decision-making.

## Risk Hierarchy

Risk managers and administrators create and view hierarchies on the risk statement form:

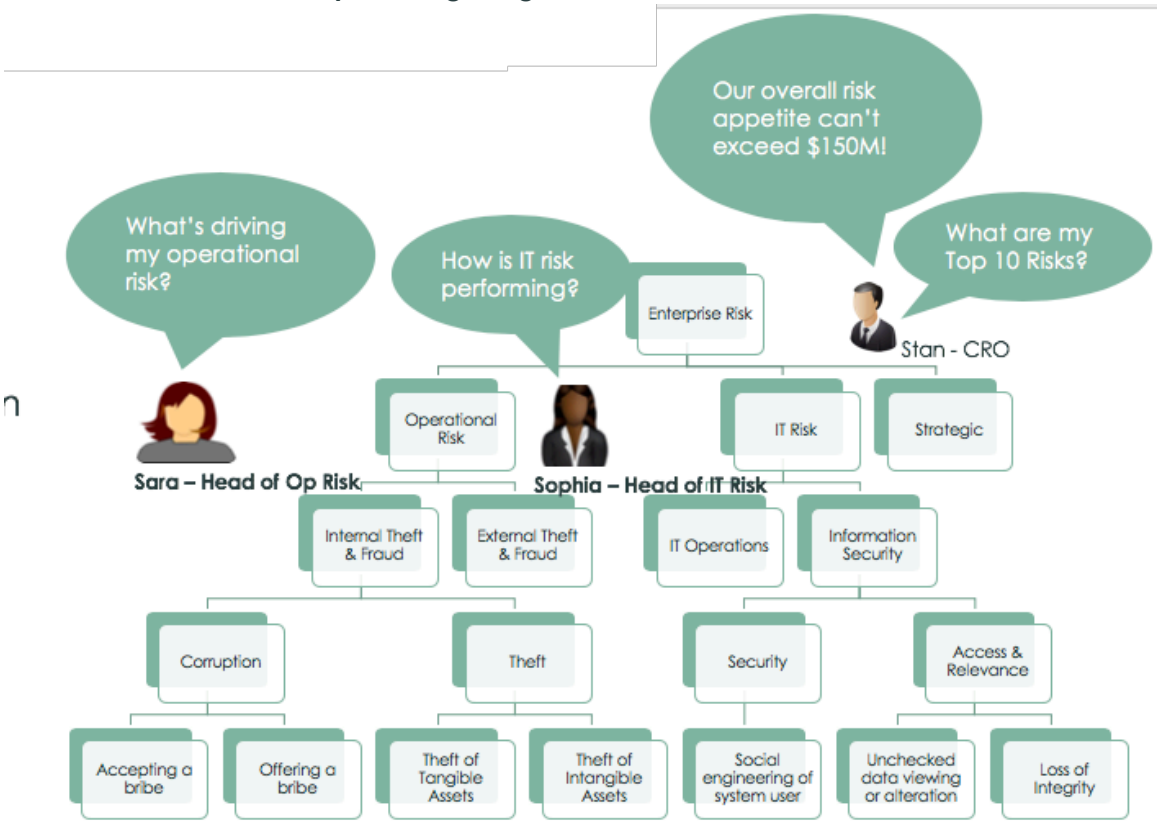
- Define a parent risk statement using the **Parent** field
- Add children risk statements using the **Risk Statements** related list

**Note:** Risk users can view the hierarchies established by the managers and administrators.

Depending on the risk areas, different people in the organization own and manage their own risks. However, top-level risk scores take into account the score of all the risks below it. Therefore, managing all the different risk areas in a central location provides an integrated view of your organizations total risk posture.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Hierarchical risk taxonomy showing integrated view of risk




## Translate quantitative risk scores to qualitative values

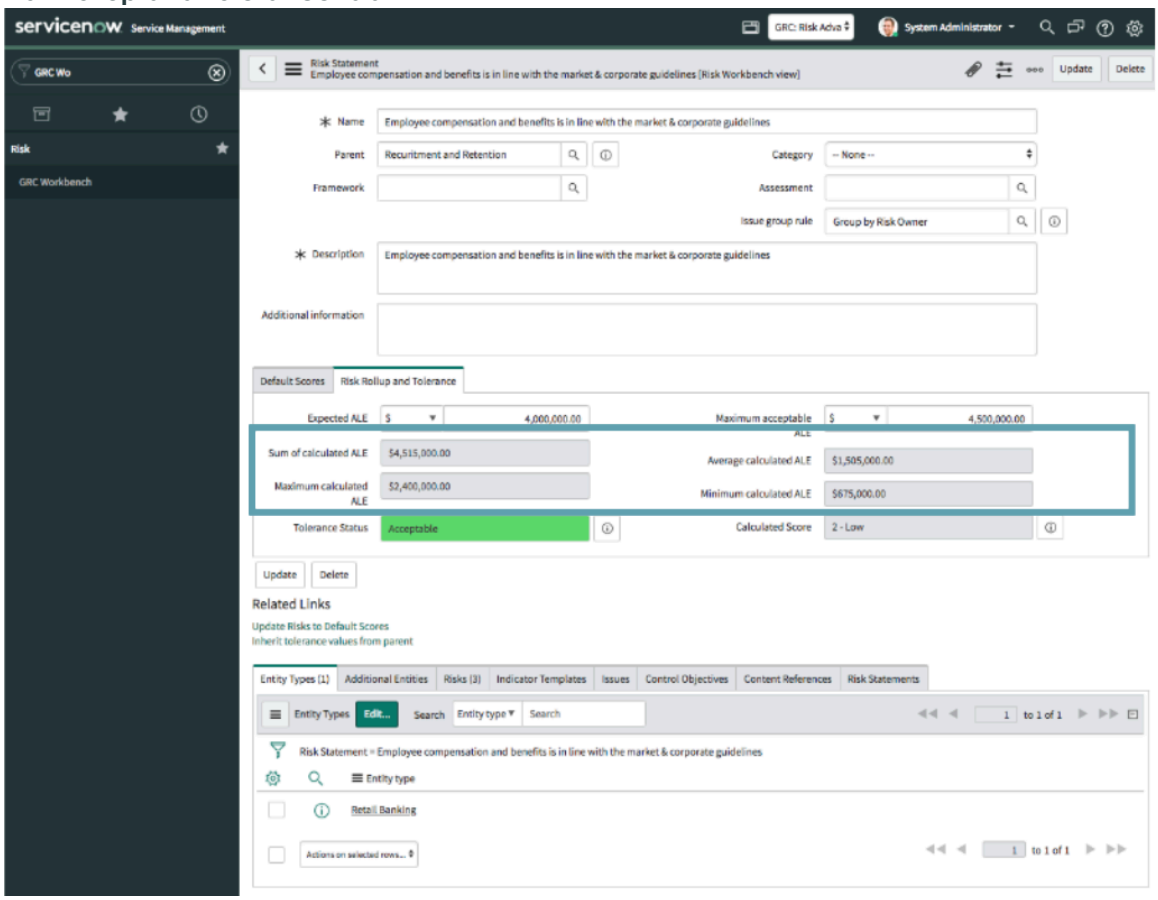
The **Tolerance Status** and the **Calculated Score** are based on the Calculated Annual Loss Expectancy (ALE) of the underlying risks:

- Sum of calculated ALE
- Average calculated ALE
- Maximum calculated ALE
- Minimum calculated ALE

**Note:** Only risks in the **Monitor** state can contribute to the risk statement scores.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Risk Rollup and Tolerance tab




### Association of entities at any level of a risk statement

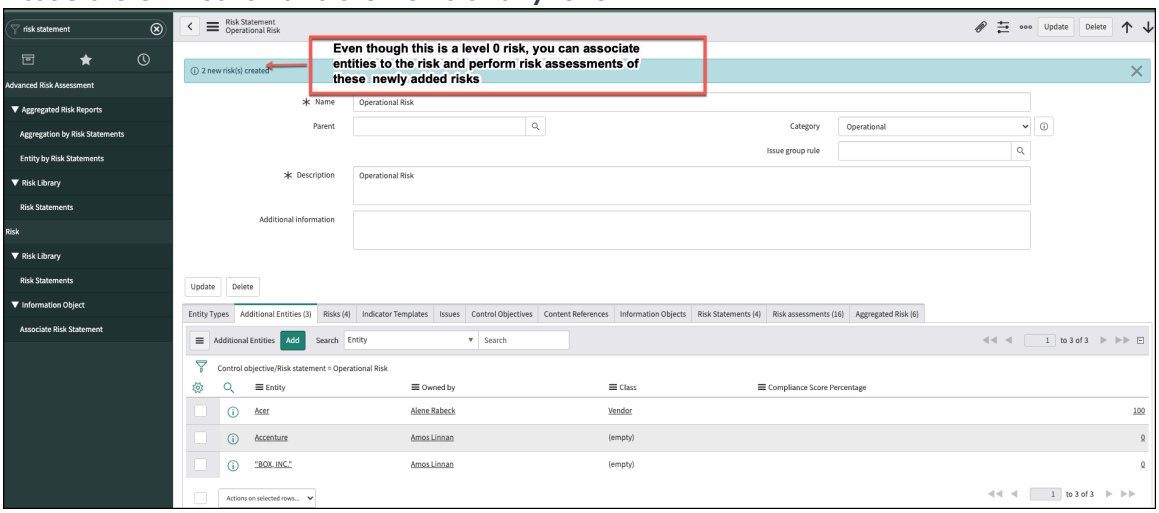
You can associate entities, entity types, and indicator templates, at any level of the risk statement hierarchy. Creating this association is useful for risk managers while assessing risks.

All organizations maintain a standardized risk taxonomy. This taxonomy is organized into hierarchies and sub-hierarchies that enable the right level reporting of risk to the appropriate stakeholders. Also, depending on the user who is assessing the risks, the level at which the risk may be assessed is different. For example, enterprise risks are assessed at the top level while detailed risk and control assessments are done at the bottom-most level of the risk hierarchy. With the latest release, users can now associate entity types or entities along with indicator templates at any level of risk statement hierarchy. Therefore, if a customer wants to perform a top-down risk assessment, they can do so by mapping the company to the top-level risk statement hierarchy. They can also perform the traditional bottom-up risk assessment by applying the lowest risk statement to the business units or lines of business. The bottom-most or lowest level is also known as the leaf level. This flexibility to associate entities to risk at any level is useful for enterprise risk managers as it helps them perform the top-down risk assessments.

The following figure shows the risk statement form where users can associate entities to create risks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Associate entities to risk statements at any level




## Manage classic risk assessments

Risk assessments are surveys to determine risk. The Risk Assessment Designer provides a single interface that users can use to create, and edit attestations, as well as change scoring parameters.

The question bank offers a library of questions for various categories, so you do not have to build each questionnaire from scratch. Risks start in a **Draft** state then move to **Assess**, which sends a notification to the Assessment respondents.

**My Assessments** is contained in the **Risk Register** module and contains active assessments for which you are the respondent. The assessments appear in a list with a single assessments record per risk.

**All Assessments** is contained in the **Risk Register** module and contains all active assessments. The assessments appear in a list with a single assessments record per risk.

Risk managers can create a new set of questions for each risk statement.

In classic risk assessment, the scores do not automatically roll up. Whenever a risk statement is created, the default scores are manually entered by the risk administrator. All the risks that are created from a risk statement inherit the scores defined in the risk statement.

## Risk indicators, control indicators, and indicator templates

Indicators are an important tool used to manage your organization's risks. Indicators collect data to monitor controls and risks, and to collect audit evidence. Indicators monitor a single control or risk. They are used to enhance and facilitate the monitoring, mitigation, and reporting of risks.

## Indicators

Indicators are useful when you want to know if your organization is compliant before you do an audit. If certain controls are non-compliant, indicators help you identify them and enable you to correct them. Continuous monitoring involves activities related to identifying and creating key risk and control indicators. Indicators are of the following types:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Manual: Manual indicators are used for data that cannot be retrieved from a ServiceNow instance because it comes from an external system, such as customer data from a third-party sales system.
- Basic: Basic indicators are automated indicators based on an indicator source. The indicator source specifies a table and a frequency at which the scores from this table are saved.
- Scripted: Scripted indicators use a custom script to collect the data.

The *GRC indicator nightly run* job executes the indicators. When an indicator is run, you have the option to collect supporting data. Supporting data refers to the evidence that is collected when an indicator is run. Supporting data or information can be collected for the indicators through automatic data collection or manual tasks.

Indicators yield results when the indicator tasks are closed. Those results are then used to create issues for controls, update risk scores, and provide supporting information for audit activities and control testing. Starting with version 10.1, the system displays the actual historical data for the supporting data records from the indicator results or indicator tasks. For more information on how to create the various types of indicators, see:

- Create and run a manual risk indicator in the Risk Workspace
- Create and run a basic risk indicator in the Risk Workspace
- Create and run a scripted risk indicator in the Risk Workspace

## Indicator templates

Indicator templates enable you to create multiple indicators for similar controls or risks. You can either use an indicator template to create indicators or you can create independent indicators. Even if you use an indicator template to create an indicator, you can modify or override the details of the indicators.

## Manage risk issues and remediation

Issues can be created manually to document audit observations or remediations, or to accept any problems. They are automatically generated from indicator results, attestation results, or control test effectiveness.

Various types of issues are created under the following conditions:

Issue

Created when an indicator fails

Control issue

Created when a control attestation is completed indicating that the control is **Not implemented**

Control test issue

Created when a control test is closed complete with the control effectiveness set to **Ineffective**

Other issue

Created by the user manually

Remediating an issue marks an intention to fix the underlying issue causing the control failure or risk exposure. Accepting an issue marks an intention to create an exception for a known control failure or risk. Controls that are **Accepted** remain in a non-compliant state until the

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

control is reassessed. In this way, the issue can be used to document observations during audits.

## Configuring Risk Management

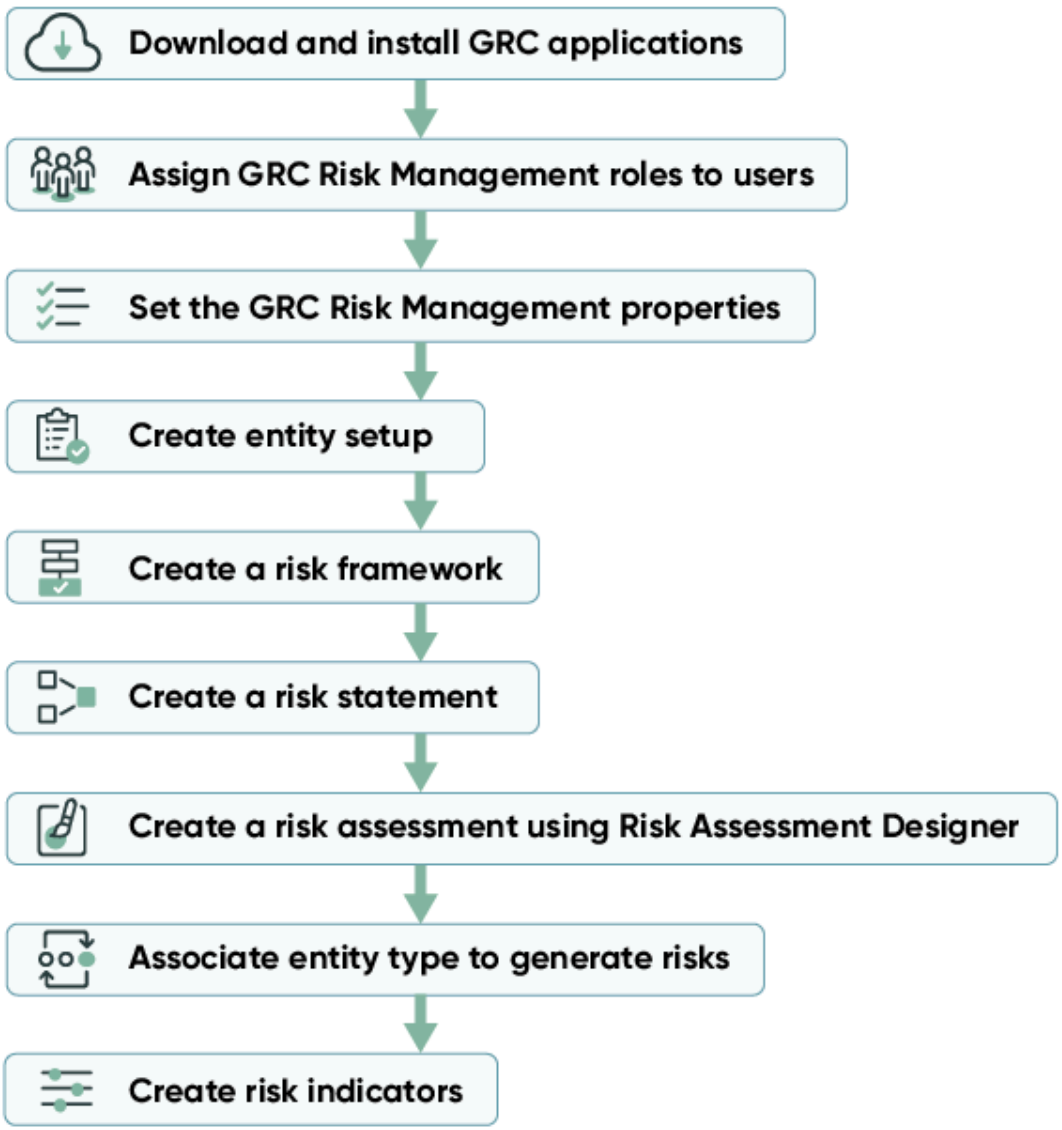
Configure the Risk Management application to use the features it provides for the complete risk management of your organization.

### Risk Management implementation

Use the steps in the Risk Management application checklist to download the Risk Management from the ServiceNow Store, and get it ready for operation. Mandatory and optional setup steps, as well as an implementation checklist are provided to simplify the setup.

The flow of mandatory steps in the checklist is illustrated here.

**Risk management implementation checklist**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Download Risk Management

Before you run GRC: Risk Management (sn_risk) in your instance, you must download it from the ServiceNow Store.

**Before you begin**
Role required: admin

**Procedure**

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

### Install Risk Management

You can install the Risk Management application (com.sn_risk) if you have the admin role. The application includes demo data and installs related ServiceNow® Store applications and plugins if they are not already installed.

**Before you begin**

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.
- Risk Management requires the following plugins. Ensure that these plugins are activated before you install Risk Management .

  Required ServiceNow plugins

  GRC Risk Management dependencies

  Installs all the dependent plugins required to support the GRC Risk Management application.

- Risk Management requires the following ServiceNow Store applications. Ensure that these applications are installed before you install Risk Management .

  Required ServiceNow Store applications

  GRC Profiles

  The GRC: Profiles application is a set of common components shared by the GRC suite of applications. The application includes common architecture, issue management, and indicators.

Role required: admin

**About this task**
The following items are installed with Risk Management:

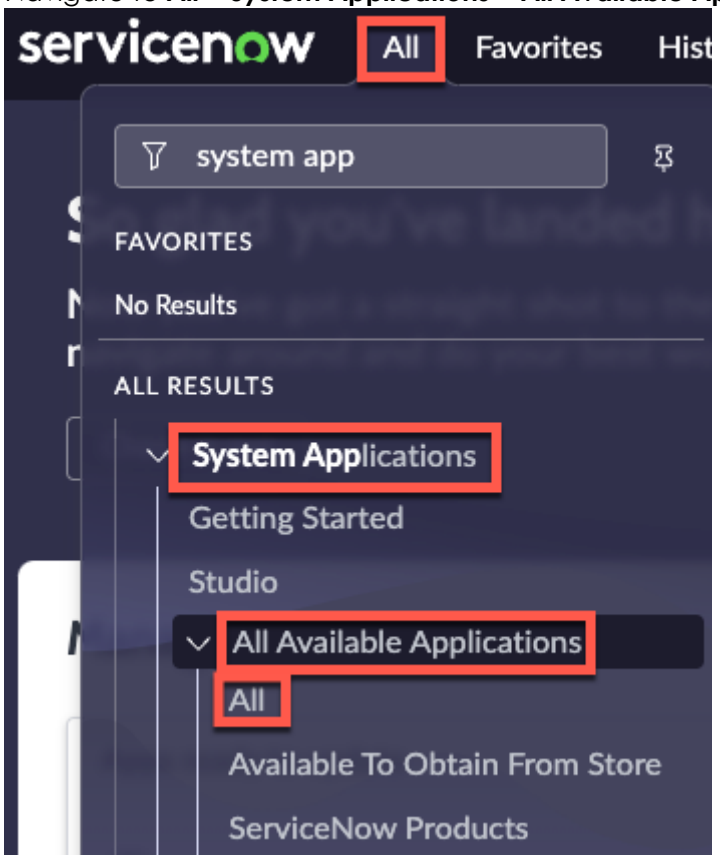
- Plugins
- Store applications
- Roles
- Scheduled jobs
- Tables

For more information, see Components installed with Risk Management.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.




2. Find the  Risk Management  application (com.sn_risk) using the filter criteria and search bar.

   You can search for the application by its name or ID. If you cannot find the application, you might have to request it from the ServiceNow Store.

   Visit the  ServiceNow Store  website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the  ServiceNow Store version history release notes .

3. In the Application installation dialog box, review the application dependencies.

   Dependent plugins and applications are listed if they will be installed, are currently installed, or need to be installed. If any plugins or applications need to be installed, you must install them before you can install .

4. Optional:  If demo data is available and you want to install it, select the **Load demo data** check box.
   Demo data comprises the sample records that describe application features for the common use cases. Load the demo data when you first install the application on a development or test instance.

   **Important:** If you don't load the demo data during installation, it's unavailable to load later.

5. Select **Install**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Setup checklist for the Risk Management application

This checklist includes the set up tasks that you are required to complete in your Now Platform® instance. When you have completed these tasks, the base system is ready for operation.

## Before you begin

Role required: sn_risk.admin

Consider creating and printing a PDF of this checklist topic. You can then check off tasks as you complete them. To generate a PDF, click the **Save As PDF** icon and at the top of the topic and click **Selected topic**.

### Risk Management application checklist

| Item | Checklist |
|---|---|
| ☐ | A user with the sn_risk.admin role, can<br>• define and modify the risk criteria<br>• configure the risk properties<br>• create assessments<br>• modify the existing assessments<br>• assign roles<br><br>For details, see Risk Management Administration. |
| ☐ | A user with the sn_risk.admin role, can also assign roles. For details, see Roles installed with Risk Management |
| ☐ | A risk manager, with the sn_risk.manager role, needs to manage numerous risk statements. To achieve this goal, the risk framework must be defined. For details, see Create a risk framework and associate risk statements to it. |
| ☐ | A risk manager, with the sn_risk.manager role, must create a risk statement to group risks logically. For details, see Create a risk statement |
| ☐ | A risk administrator or a risk manager can create a risk assessments using the Risk Assessment Designer. For details, see Create a risk assessment using the Risk Assessment Designer. |
| ☐ | Risk administrators and risk managers can create risk indicators. Risk indicators monitor changes in the levels of risk exposure and contribute to the early warning signs that enable organizations to report risks, prevent crises and mitigate them in time. For details, see Create a risk indicator. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Risk Management application checklist (continued)

| Item | Checklist |
|---|---|
| ☐ | Risk administrators and risk managers can create entities manually, rather than generating them from the entity types. For details, see Create independent entities |
| ☐ | Risk administrators and risk managers must create and edit entity types and map them to existing ServiceNow® tables for which you must track compliance. Entities are assigned to control objectives and risk statements, which generate controls and risks for every entity type. For details, see Generate risks and controls from entity types |

## Setup checklist for GRC Advanced Risk

Use the following checklist to get a high-level overview of the basic configurations available with the Advanced Risk application.

### Before you begin

Role required: sn_risk.admin

Consider creating and printing a PDF of this checklist topic. You can then check off tasks as you complete them. To generate a PDF, click the **Save As PDF** icon and at the top of the topic and click **Selected topic**.

### Advanced Risk application checklist

| Item | Checklist |
|---|---|
| ☐ | Risk managers can create hierarchies that include different types of risk (operational risk, IT risk, or strategic risk). Once the underlying risks are assessed, the risk scores are automatically rolled up across the risk statement hierarchy, providing better tactical and strategic decision-making. For details, Risk hierarchy and scoring. |
| ☐ | Risk managers must define the risk statement hierarchy and associate child risk statements to parent to create a risk hierarchy. For details, see Define risk statement hierarchy |
| ☐ | Risk rollups are critical to display the accurate risk ratings. Risk administrators can define the rollups and hierarchy. For details, see Risk score rollup in Advanced Risk Assessment |
| ☐ | Risk events are potential or actual financial and non-financial losses, near misses, and gains that occur within an organization. Risk administrators can integrate risk events with other applications to facilitate reporting |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Advanced Risk application checklist (continued)**

| Item | Checklist |
| --- | --- |
| | of risk events. For details, see Manage risk events |
| ☐ | With GRC Advanced Risk Assessment, create an integrated risk platform. Risk administrators can configure detailed risk assessment options. For details, see Advanced Risk Assessment |

### Download Advanced Risk

Before you run Advanced Risk in your instance, you must download it from the ServiceNow Store.

**Before you begin**
Role required: admin

**About this task**
GRC Risk Advanced provides access to the following features:

- Manage risk events
- Risk hierarchy and scoring

**Procedure**

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

## Risk Management detailed setup

Set up Risk Management so that you can use the features such as risk assessments, risk events, and other capabilities of the GRC Risk Management application.

To setup Risk Management:

1. Download Risk Management: Before you run GRC: Risk Management (com.sn_risk) in your instance, you must download it from the ServiceNow Store.
2. Download Advanced Risk: Before you run Advanced Risk in your instance, you must download it from the ServiceNow Store.
3. Mobile experience for GRC Risk Management: As a risk manager, use your Android or iOS mobile device to manage your work.
4. Quick start tests for Risk Management: Validate that Risk Management still works after you make any configuration change, such as apply an upgrade or develop an application. Copy and customize these quick start tests to pass when using your instance-specific data.

### Quick start tests for GRC Advanced Risk

Validate that Advanced Risk still works after you make any configuration change, such as apply an upgrade or develop an application. Copy and customize these quick start tests to pass when using your instance-specific data.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## GRC Advanced Risk

GRC: Advanced Risk quick start tests require activating the GRC: Advanced Risk plugin (com.sn_risk_advanced) and loading the demo data.

### GRC: Advanced Risk test suite

| Test | Description | Release version |
|---|---|---|
| GRC: Create a Risk Event | Validates the creation of risk events. | New York |
| GRC: Create Risk Statement Hierarchy | Validates if the risk statement has a parent field so that the hierarchy can be maintained among risk statements | New York |
| GRC: Reject a Risk Event | Validates the rejection functionality the risk event | New York |
| GRC: Request more info - Risk Event | Validates the Request more information functionality before approving the risk event | New York |
| GRC: Create risk assessment scope | Creates different types of factors like manual factors, query factors, and automated scripted factor. It creates a Risk Assessment Methodology and associates the factors to the different assessment types in the Risk Assessment Methodology. It creates the Risk Assessment scope for the Risk Assessment Methodology. that has been set up.<br><br>**Note:** While running ATF Tests, it is recommended to increase the test runner timeout from 120 seconds to approximately 240 seconds in the Test Runner Properties. | Orlando |

To learn more about Advanced Risk, see Download Advanced Risk

### Configure Risk Management

Administrators in the global domain can set properties to determine how the system defines the Risk Management application.

**Before you begin**
Role required: sn_risk.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** Administrators in domains lower than the global domain can view the Properties screen, but cannot modify the settings.

### Procedure

1. Navigate to **All** > **Risk** > **Administration** > **Properties**.
2. Fill in the fields on the Risk Management Properties form.
   See Properties installed with Risk Management for property descriptions.
3. Click **Save**.

Related topics

Properties installed with Risk Management

### Risk Management Administration

Using the Risk Management application, administrators can customize risk categories, risk criteria, risk management properties, and risk assessment types.

## Risk criteria

Risk criteria are the scoring values attributed to the likelihood that a risk occurs, and the impact to your organization if the risk does occur.

Risk criteria thresholds define a high/likely or low/unlikely score as shown:

#### Risk criteria thresholds

| Likelihood | Impact | Scores |
|---|---|---|
| 1 = Extremely Unlikely | 1 = Very Low | 0-5 = Very Low |
| 2 = Unlikely | 2 = Low | 6-10 = Low |
| 3 = Neutral | 3 = Moderate | 11-15 = Moderate |
| 4 = Likely | 4 = High | 16-20 = High |
| 5 = Extremely Likely | 5 = Very High | 21-25 = Very High |

#### Risk properties

| Name | Description |
|---|---|
| A list of tables that are available in the **Applies to** field on forms | If this field is blank, all tables are available on the various forms for Entity Types, Entities, and Risks. Defines a comma-separated list of tables that are available in the **Applies to** field on the Entity Type, Entity, and Risk form. Add *.extended* after the table name to include all extended tables. |

## Assessment types

Risk managers can create a new set of questions for each risk assessment. See Create an assessment type.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Quick start tests for Risk Management

Validate that Risk Management still works after you make any configuration change, such as apply an upgrade or develop an application. Copy and customize these quick start tests to pass when using your instance-specific data.

GRC: Risk Management quick start tests require activating the Risk Management plugin (com.sn_risk) and loading demo data.

#### GRC: Risk Management Quick Start Tests test suite

| Test | Description | Release Version |
|---|---|---|
| GRC: Create Profile | Validate profile creation. | Madrid |
| GRC: Create Risk | Validates risk creation. | Madrid |
| GRC: Create Control | Validates control creation. | New York |
| GRC: Create Control Objective and Generate Controls | Validates control objective creation and associates profiles to generate controls. | New York |
| GRC: Create Issue | Validates issue creation | New York |
| GRC: Accept an Issue | Validates all the states of an issue till it is closed by accepting the issue. | New York |
| GRC: Remediate an Issue | Validates issue cannot be closed be with an open remediation task. | New York |
| GRC: ATF Flow for Indicator (Manual): | Create an indicator template with type manual and associate a control objective to it. Execute one of the indicators thus formed. Mark the state of the indicator task created as closed and result as failed. The associated control will become non- compliant and an issue will be generated. | New York |
| GRC: ATF flow for Indicator (Basic) | Create an indicator template with type basic and result as failed. Associate a control objective to it and give the supporting data. Execute one of the indicators thus formed. The associated control will become non- compliant and an issue will be generated. | New York |
| GRC: ATF flow for indicator (Script) | Create an indicator template with type script and enter a script and set the value of result.passed and result.value. Associate | New York |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**GRC: Risk Management Quick Start Tests test suite (continued)**

| Test | Description | Release Version |
|---|---|---|
| | a control objective to it. Execute one of the indicators. The associated control will become non-compliant and an issue will be generated. | |

Related topics

Quick start tests

## Set up checklist for the GRC Mobile application

The following checklist includes the set up tasks that you are required to complete in your Now Platform® instance and on your mobile device. Complete these set up tasks prior to using the GRC Mobile application to view the Risk Management application on your mobile device.

### Before you begin

As an option, print this checklist and use it to guide you through the set up tasks that are required for the GRC Mobile application. Verify that each item on the list is completed so that you can log in to the GRC Mobile application and add a Now Platform instance.

Time to complete this task: 15-20 minutes.

Roles required: admin, sn_risk.manager

**GRC Mobile application checklist**

| Item | Description |
|---|---|
| ☐ | As a user with the admin role, verify that you have the GRC core applications installed on a Now Platform instance. This is the Now Platform instance that you view on your mobile device.<br><br>**Note:** The GRC core applications and the Now Platform instance should be from the same family release.<br><br>1. To verify the GRC: GRC Profile Dependencies core application is installed on your instance, navigate to **Plugins** and search for GRC Profile.<br>2. If the GRC Profile core application is not already installed, click **Install** to install it.<br>3. After the GRC Profile application is installed, install either the Policy and Compliance Management core application, or the Risk Management core application, or both the Policy and Compliance Management and Risk Management applications. These are the two GRC applications that you can view with the GRC Mobile application.<br><br>If not visible in your instance, all of the GRC core applications are available from the ServiceNow Store. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**GRC Mobile application checklist (continued)**

| Item | Description |
|---|---|
| | For more information about getting entitlement, downloading, and installing the GRC core applications, see GRC and the ServiceNow Store.<br><br>When you install the GRC core applications, the dependency plugins for the GRC Mobile application, (com.glide.sg and com.glide.sg.agent_native_client) are also automatically installed.<br><br>To verify that these dependency plugins are installed and activated:<br><br>**1.** Navigate to **Plugins**.<br>**2.** Search for the plugin IDs (com.glide.sg and com.glide.sg.agent_native_client).<br>**3.** If they are not activated, activate these plugins. |
| ☐ | As a user with the admin role, verify that you have the GRC mobile app installed on the Now Platform instance that you want to view on your mobile device.<br><br>**Note:** The GRC mobile app and the Now Platform instance should be from the same family release.<br><br>For more information about getting entitlement, downloading, and installing the GRC Mobile application, see GRC and the ServiceNow Store. |
| ☐ | As a user with the admin role, in your Now Platform instance verify that you have assigned mobile users with the required Now Platform roles.<br><br>**1.** To view the roles that are assigned to a user, navigate to **Users and Groups** > **Users**.<br>**2.** Select the user name followed by the roles related list. All roles assigned to this user are displayed.<br>**3.** Verify a user is assigned, or assign a user with the IT Infrastructure Library role (itil). Users with the itil role can create, open, and update records. Only users with the itil role can have tasks assigned to them.<br>**4.** Verify a user is assigned, or assign a user with the risk manager role (sn_risk.manager). This role is automatically added when you assign the itil role.<br>**5.** Verify you have created any required assignment groups and assigned mobile users to these groups.<br><br>**Note:** If you have multiple users for the mobile application, you alternatively can assign the sn_risk.manager role to a group. Each user you add to the group inherits this role.<br><br>For more information on users and assigning roles to users and groups, see Create a user. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**GRC Mobile application checklist (continued)**

| Item | Description |
|---|---|
| ☐ | As a mobile user with the sn_risk.manager role, verify that you have installed the most current ServiceNow® Agent application on your mobile device.<br><br>**Agent mobile app**<br><br>The most current Agent app is available on the Apple iOS App Store and the Google Play Store. |
| ☐ | As a user with the sn_risk.manager role, verify notifications are enabled on your mobile device and in your Now Platform instance.<br><br>Notifications inform you when critical pending approval requests are assigned to you or to your assignment group. To assist you with timely remediation, after you enable notifications, click on a notification in the GRC Mobile application and navigate directly to the record.<br><br>To enable notifications in your Now Platform instance so they are displayed on your mobile device, follow these steps.<br>1. Verify you have downloaded and installed the GRC Mobile application on your Now Platform instance.<br>2. In System Settings in your Now Platform instance, under Notifications, verify you have enabled the **ServiceNow Mobile Application**.<br><br>For more information about setting notifications, see "User notification preferences in Core UI" on the Setting notification preferences in Core UI.<br><br>Now Platform notifications are also displayed on the messages screen on your mobile device. Verify that notifications are also enabled in the settings of your mobile device. |

You have successfully set up your mobile device and the Now Platform for the GRC Mobile application. The next step is to log in to your Now Platform instance with the ServiceNow Agent app on your mobile device.

## Risk appetite setup

You can configure the risk appetite feature in the Advanced Risk application.

Follow the order of the tasks to configure the risk appetite feature in the Advanced Risk application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Configure a risk appetite and tolerance in Advanced Risk

Set up the advanced risk assessment properties so that you can configure and customize the risk appetite and tolerance in the Advanced Risk application.

## Before you begin

Role required: sn_risk.admin

## Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Properties**.
2. Set the property values that are described in the following table.

**Advanced risk assessment properties**

| Property | Description |
|---|---|
| Migrate to Advanced Risk Assessments<br><br>sn_risk_advanced.hide_risk_legacy_lifecycle | Option to migrate to the advanced risk assessments. Select **Yes** to use the risk appetite feature. |
| Define risk appetite as<br><br>sn_risk_advanced.risk_appetite_scale | Option to select the risk appetite type:<br>◦ **Risk appetite only (1-point scale)**: Uses only the risk appetite. The risk appetite field is available on the risk statement, risk, and entity form. The risk appetite status is calculated based on this property selection.<br>◦ **Risk appetite and risk tolerance (2-point scale)**:Uses both the risk appetite and tolerance. The risk appetite and risk tolerance fields are available on the risk statement, risk, and entity form. The risk appetite status is calculated based on this property selection.<br>◦ **None**: Don't want to use the risk appetite.<br><br>**Note:** Only one property between the **Define risk appetite as** and **Express risk appetite in** can be configured at a time. Configure a property first, save it, and then configure the other property. |
| Express risk appetite limits in<br><br>sn_risk_advanced.risk_appetite_analysis | Option to select risk appetite scale:<br>◦ **Qualitative terms only**: Defines the risk appetite in qualitative terms only. Your risk appetite is based on the appetite scale such as low, medium, or high. The risk ratings are compared with the qualitative appetite and tolerance to calculate the qualitative appetite status.<br>◦ **Quantitative terms only**: Defines the risk appetite in quantitative terms only. A quantitative risk appetite can be measured and expressed using numerical |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Property | Description |
| --- | --- |
| | values. For example, an organization decides to have $1000 (US dollars) as a target non-performing asset (NPA) for this year. The organization can define $1000 (US dollars) as a quantitative risk appetite. The annual loss expectancy values are compared with the quantitative appetite and tolerance to calculate the quantitative appetite status.<br>◦ **Both**: Defines the risk appetite in both qualitative and quantitative terms.<br>**Note:** Only one property between **Define risk appetite as** and **Express risk appetite in** can be configured at a time. Configure a property first, save it, and then configure the other property. |
| Number of days before which an email should be sent to review risk appetite<br><br>sn_risk_advanced.risk_appetite_review_notification | Notification email scheduler to send an automated email notification to the risk statement owner before the next review date. |

3. Select **Save**.

### Set up a risk appetite scale

Set up a risk appetite scale in the Advanced Risk application to define the qualitative risk appetite within your organization.

#### Before you begin
Role required: sn_risk.admin

#### About this task
Use a risk appetite scales to define the qualitative risk appetite on the risk statement, entity, and risk records. The risk appetite scales that are shipped by default are as follows:

- **1-Averse**
- **2-Minimalist**
- **3-Cautious**
- **4-Open**
- **5-Hungry**

#### Procedure
1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Risk Appetite Scales**.
2. Select **New**.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Risk Appetite Scale form

| Field | Description |
|---|---|
| Name | Name of the risk appetite scale. For example, Hungry. |
| Active | Option to enable the appetite scale. You can't delete a risk appetite scale. Instead, you make it as inactive. This option is automatically selected.<br>**Note:** When you make a risk appetite scale active or inactive, it affects multiple records, such as related risk assessments, entities, risk statements, and risks. |
| Description | Brief description about the appetite scale. |
| Value | Value of the risk appetite scale. This field defines a numerical value of the risk appetite scales.<br>**Note:** Any change in the risk appetite value affects multiple records, such as related risk assessments, entities, risk statements, and risks. |
| Display order | Order of the risk appetite scale. This field enables you to set a sequence in which the risk appetite scale appears. |

4. Select **Submit**.

## Change a risk appetite status

Change the default name, color, and icon that appear for the risk appetite status in the Advanced Risk application.

### Before you begin
Role required: sn_risk.admin

### About this task
Use the risk appetite status to define the final risk status of the entities, risks, and risk statements that are based on the defined risk appetite. The appetite status helps you to monitor the risk and to define further actions to bring the risk within the appetite.

The risk appetite statuses that are shipped by default are as follows:

- **Outside appetite**
- **Outside tolerance**
- **Within appetite**

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** A risk appetite status can't be deleted but can be retired or created. When you create a risk appetite status, customization of the application is required to enable it for status computation.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Risk Appetite Status**.
2. Open the risk appetite status that you want to change.
3. On the form, fill in the fields.

**Risk Appetite Status form**

| Field | Description |
|---|---|
| Name | Name of the risk appetite status. For example, Outside appetite. |
| Color for risk appetite status | Color that appears for the risk appetite status.<br>**Note:** To make this change on the workspace view for the risk, entity, and risk statement, you must perform some additional steps. For more information about these additional steps, see KB0867184. You must log in to the Now Support to view the Knowledge Base articles. |
| Icon | Icon that appears for the risk appetite status.<br>**Note:** To make this change on the workspace view for the risk, entity, and risk statement, you must perform some additional steps. For more information about these additional steps, see KB0867184. You must log in to the Now Support to view the Knowledge Base articles. |

4. Select **Submit**.

## Modify Advanced Risk messages

Modify the messages displayed on the risk assessment form using the Advanced Risk application. Modifying system messages enables personalized and consistent messaging for users, aligning with their preferences and specific requirements.

### Before you begin

Role required: admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **System UI** > **Messages**.
2. To filter all the advanced risk assessment messages, select the Key column and search for `advanced_risk_assessment_component`.
   Messages related to advanced risk assessment appear.
3. Select the message that you want to modify.
4. **Note:** Make sure you are not modifying the **Key** field.

   Modify the message text in the **Message** field.
5. Select **Update**.

## Create related list groupings in Advanced Risk

Simplify the groupings of related lists on a record page and customize them to your specific needs, assigning meaningful names in the process. This configuration enhances readability and user experience when interacting with the forms.

### Before you begin

Role required: admin or sn_grc_workspace.record_view_admin

### About this task

On a form, there can be numerous related lists that can occasionally result in a cluttered view. To streamline the display, you have the option to select and configure the related lists you want to see on the form. By default, the ability to configure the related lists is given for the following tables:

- Calculated Metric Definition table
- Metric Definition table

While you can select any table and configure the related lists for that table, as an example, this procedure describes how you can create groupings for the Metric Definition table. Apart from the related lists, you can also specify a UX page that you want to display under a group.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Record View Configuration**.
2. Select **Risk workspace configuration**.
3. In the Table configurations related list, select **Metric Definition**.
4. In the Group configurations related list, select **New**.
5. On the form, fill in the fields.

#### Group configuration form

| Field | Description |
|---|---|
| Table configuration | Name of the table for which you're configuring the related list. This field is automatically set. |
| Name | Name of the group that is displayed on the related list of the form. For example, you can provide a name such as `Risk` for |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | grouping risk-related objects, such as risks and risk statements. |
| Active | Option to indicate if the configuration is active. |
| Order | Order number of the group on the form.<br>**Note:** If you want to display the order before the Details tab, then the order number must be less than or equal to `100`. |
| Condition | Conditions that must be met to be displayed on the form. For example, you can specify if a record is active, only then it must be displayed on the form. |

6. Select **Submit**.
7. In the Group configurations related list, select the entry you created.
   a. In the Group entries related list, select **New**.
   b. On the form, fill in the fields.

**Group entry form**

| Field | Description |
|---|---|
| Group configuration | Group for which the related list is created. For example, in this procedure, the group for which you're configuring the entry is **Risks**. |
| Order | Order of the entry on the UI page. |
| Application | Application for which the related list is being created. This field is automatically set to **GRC: Risk Management Workspace**. |
| Active | Option to indicate if the entry is active. |
| Type | Choice to indicate the type of item the group contains. The choices are as follows:<br>▪ **UX page**<br>▪ **Related list** |
| Related list | Related list that you want must appear under the group. This option appears only when the **Type** field contains **Related list**. |
| Screen | Specific variation or version of a page. This option appears only when the **Type** field contains **UX page**. |

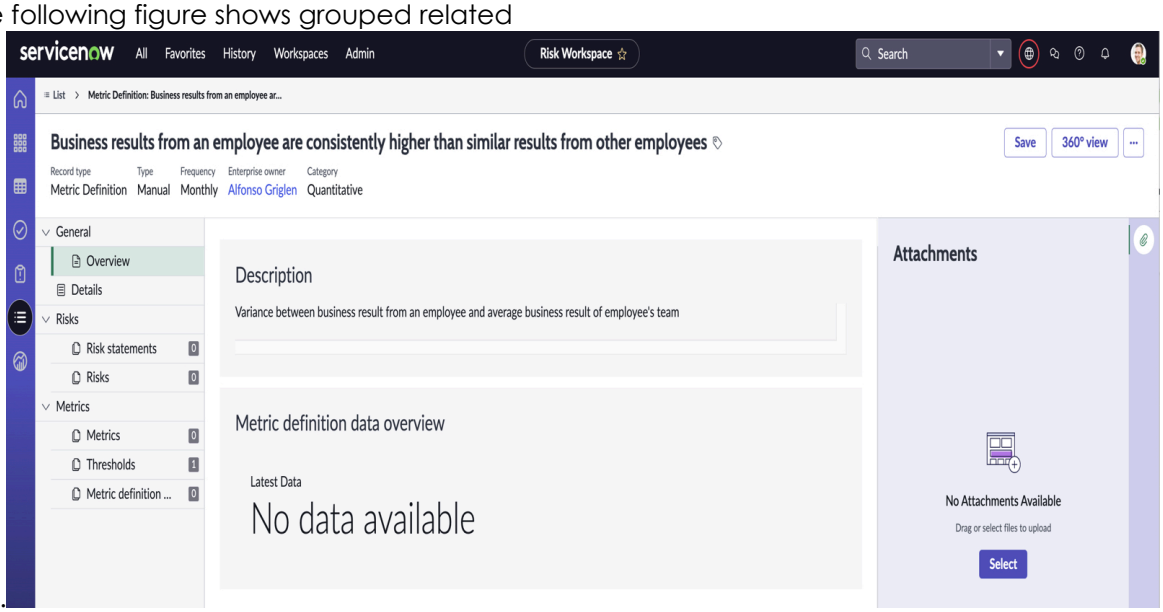
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Route | The path of the UX screen. This option appears only when the **Type** field contains **UX page**. |

**c.** Select **Submit**.

**Result**

The following figure shows grouped related lists.




## Integrating Risk Management with other applications

Extend the capabilities of Risk Management such as Advanced Risk Assessment and help other applications with risk identification and risk assessments.

Advanced Risk Assessment goes outside of Governance, Risk, and Compliance to help other applications such as APM and Project Portfolio Management identify and assess their risks and manage their life cycle.

Manage your project risks by using the project risk assessment capability. This capability enables the risk administrators, projects managers, and risk owners to manage the complete project risk life cycle such as project risk identification, project risk assessment, project risk mitigation, and project risk monitoring. This feature provides efficient visibility and reporting of the project risks posture through mediums such as aggregated project risk ratings and heatmaps. The integration of with also ensures that when a project risk threatens to affect an enterprise, the risk can be easily reported to the enterprise risk team so that the necessary mitigating actions can be defined. To use this feature, ensure that you have the Project Portfolio Management application installed. You must also enable the Enable Advanced Risk PPM Integration property under Advanced Risk Assessment Administration Properties. The default setting for this property is No. Only users with it_pps_admin or risk_admin roles can enable this property.

Manage your digital risks with business applications by using the application risk management capability. This capability allows the management of the complete risk life cycle of a business application including general data collection about the application, application inherent risk assessment, applicability of the appropriate policies, regulations and controls, and implementation and monitoring of controls. The integration of the GRC workflow with the business application reduces the communication barriers and

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

reduces the information silos in the two organizations. This reduction of barriers reduces the overall effort in management of business applications. To use this feature, ensure that you have the Application Portfolio Management (APM) application, Application Portfolio Management integration with Policy and Compliance Management and Application Portfolio Management integration with Risk Management installed.

## Project Risk Assessment using Advanced Risk Assessment

Manage your project risks by using the Project Risk Assessment capability. Risk administrators, projects managers, and risk owners can manage the complete project risk life cycle by using the Project Risk Assessment capability.

As your organization grows, it is important to perform risk assessments of your projects. Because each project is unique, it is important to customize the project risk management process according to the unique project requirements. Determining the right level of project risk management process constitutes the risk management plan. The project risk life cycle consists of phases such as project risk identification, project risk assessment, project risk mitigation, and project risk monitoring.

With version 11.0.1, you can use Governance, Risk, and Compliance (GRC) Advanced Risk Assessment to assess your project risks. This feature enhances the risk management capabilities in Project Portfolio Management. The feature is integrated with a strong risk assessment engine which you can use with strong project risk management requirements. This feature also provides efficient visibility and reporting of the project risks posture by using tools such as aggregated project risk ratings and heatmaps. The integration also ensures that when a project risk threatens to affect the enterprise, the risk can be easily reported to the enterprise risk team. The enterprise risk team can then define the necessary mitigating actions.

## Benefits of the GRC and Project Portfolio Management integration for managers

Using this integration, Project Managers can do the following activities:

- Identify the risks from a standard risk taxonomy.
- View the risks for their projects within the Project form.
- Identify and assess the risks from the Project form itself.
- Assess the inherent and residual risks.
- Elevate a project risk to an enterprise risk if the risk impacts the enterprise.
- Calculate the roll-up risk scores across projects, programs, and portfolios so that the stakeholders can view this information.
- Monitor the risk posture of a project through risk aggregation.

  **Note:** Only the project risks that are assessed contribute to the final risk scores.

- View the heatmap of the risks as well as understand the mitigating actions.
- View the Project Risk Overview dashboard to get an overall risk posture.

Enterprise Risk Managers also benefit from the integration. They can do the following activities:

- View the project risks that affect the enterprise and take necessary action.
- Get an overall view of the enterprise-level risks and their nature at all levels.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Use case for the GRC and Project Portfolio Management integration

To understand the use case for this integration, consider the following scenario. An organization can have multiple projects. Some projects are complex and some are less complex. Risk management of complex projects may be aligned to ISO 31000 risk assessment standards. Complex projects require various activities such as risk identification, assessment, response, and monitoring. Less complex or simpler projects might require only simple assessments. The integration between Project Portfolio Management and Advanced Risk Assessment supports the risk assessment of project risks.

Related topics

About Project Portfolio Management

### Workflow of project risk assessment

To understand the integration of Project Portfolio Management and Governance, Risk, and Compliance risk management capabilities, it is important to understand the workflow of project risk assessment.

Project risk assessment follows a sequence of steps. Sometimes, a risk is elevated to an enterprise risk after the risk is assessed. An enterprise risk is a risk that can cause monetary or reputational losses. It can jeopardize your ability to stay in business.

The workflow of project risk assessment is as follows:

1. A project manager identifies risks and adds those risks to a project. The manager can either create risks or add them from a library. The project manager has the it_project_manager and sn_grc.business_user roles. For more information, see Add risks for a project.
2. The project manager then initiates risk assessment for the newly added risks. In the Project Integration Configuration form, the assessors and approvers are defined for the assessment. They get an email notification to assess the risks.

   **Note:** You can only assess the risks that are in the Pending, Open, or Work in Progress state.

3. If the Project Integration Configuration form has stakeholders selected as assessors, then the project manager must manually assign the risks to the relevant stakeholder.
4. As a risk specialist, the risk assessor is notified about the new risks for assessment.

   The risk assessor can use the link in the email notification to start the assessment. Alternatively, the risk assessor can navigate to **Advanced Risk Assessment** > **Risk Assessment Tasks** > **My Tasks** to perform advanced risk assessment. See Advanced Risk Assessment.

5. In the project risk form, the project manager reviews the Risk Assessment Summary section to view the risk assessment scores.
6. If the project manager determines that the project risk has an impact on the enterprise, then the project manager can elevate the risk to an enterprise risk.

   **Note:** When a project risk is elevated to an enterprise risk, the project risk is copied from the project risk register to the enterprise risk register.

7. If a risk is elevated to an enterprise risk, the enterprise risk manager is requested to assess the risk.
8. The project manager views the enterprise inherent risk score and the enterprise residual risk score in the **Risk Assessment Summary**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

9. As part of the Project Portfolio Management workflow, if a risk materializes and an action must be taken for this risk, then the project manager can convert the risk into an issue. For more information, see RIDAC (Risk, Issue, Decision, Action, and Request Changes) record entries for a project.
10. The project manager can also view the project risk posture through the heatmap in the Risk Overview section on the project form. The heatmap displays high impact risks and high likelihood risks. With the heatmap, you can prioritize the risks that need immediate attention. The risks that are assessed contribute to the aggregated risk score. The aggregated risk score is a single score that can be reported to all the stakeholders. For more information, see Create a project.
11. View the Project Risk Overview dashboard to understand the overall risk posture of project risks and of enterprise risks. For more information, see Project Risk Overview dashboard.

**Note:** The assessor and the approver must have risk business user role (sn_grc.business_user) to perform the required tasks. If the project risks are reassessed for any reason and the scores change, then the enterprise risk assessor gets an email notification with the option to reassess the enterprise risk.

The key users and the user journey are shown in the following figures.

**Key users of Project Portfolio Management and Risk Integration**



**Project Managers**
- Own the overall project risk and need visibility into project risks
- Use the aggregated risk to understand the overall project risk posture as well as visualize their distribution on the heatmap
- Can elevate risks to enterprise risk register if they have materialistic impact to the enterprise



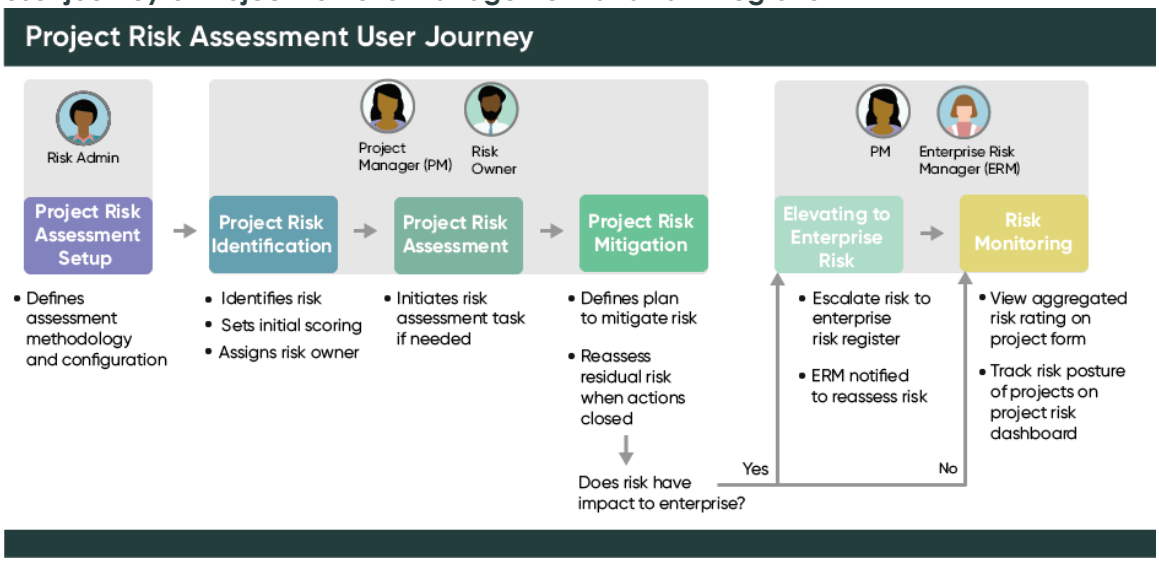
**Project Risk Owners**
- Own the specific risk and assess and mitigate it to contain it from materializing
- Use the ARA to assess the inherent risk, define actions to mitigate those risks and assess the leftover (risidual) risk to decide if further mitigating actions are required



**Enterprise Risk Managers**
- Need visibility into risks from the projects and understanding of which risks may impact the overall organization risk posture
- Can reassess project risk which may have an enterprise impact to analyze such risks and take appropriate action on them

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### User journey of Project Portfolio Management and risk integration




## Configure Project Portfolio Management and Advanced Risk integration

Use the Project Integration Configuration form to set up the risk assessment. You have to select the risk assessment methodology, the right assessors and approvers, and the formula to roll up the risk scores and show the scores at a project level.

### Before you begin

To use Advanced Risk Assessment for Project Management, do the following:

- Activate the Project Portfolio Management plugin.
- Activate the Advanced Risk plugin.
- Enable the *Enable Advanced Risk PPM Integration* property under **Advanced Risk Assessment** > **Administration** > **Properties**. This property is automatically set to **No** by default. Only users with the it_pps_admin or sn_ risk.admin roles can enable this property..

**Note:** Currently, in the Project Portfolio Management suite, advanced risk assessments are only supported for the Project Management application.

Role required: sn_risk.admin

### About this task

As the risk administrator, you can select the following on the Project Integration Configurations form:

- The risk assessment methodology (RAM).
- The approvers and assessors for both enterprise risk assessment and project risk assessment.

Two predefined RAMs are provided for Enterprise Risk Assessment and Project Risk Assessment. You can modify the default methodology or create methodologies. If you select your own risk assessment methodology, then the entity class for that methodology must be Project. For assessing project risks and enterprise risks, you can add the approvers and assessors of your choice. The risk assessment methodology for project risk is automatically selected as the methodology that is associated to the Project Portfolio Management risk table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Project Integration Configuration**.
2. Click the information icon to view the project risk integration configuration record.
3. Click **Open Record**.
4. On the form, fill in the fields.

**Project Risk Integration Configuration form**

| Field | Description |
|---|---|
| Project Risk Assessment | |
| Assessment methodology | The assessment methodology for project risk assessment. This field is automatically set to **Enterprise Assessment for Projects** |
| Assessor type | Assessor for the project risk assessment. The choices are as follows:<br>◦ Project Manager: The user assigned as the project manager of the project.<br>◦ Risk Owner: The user who is identified in the**Assigned to** field of the risk.<br>◦ Stakeholders: Stakeholders for the project.<br>**Note:** If **Stakeholder** is selected, then when the project manager assigns the assessor, all users who are added to the Stakeholders related list in the project are displayed. The project manager can select the required stakeholder. |
| Risk rollup formula | The formula used to roll up the project risk scores. The choices are as follows:<br>◦ Average<br>◦ Maximum<br>◦ Minimum<br>**Note:** Only the risks that are assessed using Advanced Risk Assessment are aggregated and have their scores rolled up. If a risk is retired, then the score of the retired risk is not aggregated. For details, see Risk score rollup in Advanced Risk Assessment. |
| Approver type | Approver of the project risk. The approver has to approve the risk assessment. The choices are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ None: No approver is necessary.<br>◦ Project Manager: The project manager is the approver.<br>◦ Stakeholder: The stakeholders for the project. |
| Enterprise Risk Assessment | |
| Assessor type | Assessor for enterprise risk. The choices are as follows:<br>◦ Project Manager: The user assigned as the project manager of the project.<br>◦ Risk Owner: The user who is identified in the**Assigned to** field of the risk.<br>◦ Group: The group to which the risk is assigned.<br>**Note:** This user must have the sn_risk.manager role. |
| Approver type | Approver for enterprise risk. The choices are as follows:<br>◦ None: When no approver is necessary.<br>◦ Project Manager: The user assigned as the project manager of the project.<br>◦ Group: The group to which the risk is assigned. |
| Days to overdue | Number of days after which an assessment is considered overdue starting from the date of initiation. The field is automatically set to **5**.<br>**Note:** The assessor gets reminder notifications before the due date approaches. The assessor and the assessor's manager get a notification after the due date passes. |
| Assessor group | The group which assesses the enterprise risk if the **Assessor type** field has **Group**. |

5. Click **Update**.

**Result**
The assessor and approver details are set.

### Assign project risks to stakeholders for assessment

Assign the project risks to the relevant stakeholder for assessment. You must manually assign the risks to the stakeholders.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: it_project_manager

### About this task
If the Project Risk integration Configuration form has **Stakeholders** selected as an assessor, then the project manager must manually assign the assessment to one of the stakeholders of the project.

### Procedure
1. Navigate to **All** > **Project** > **Projects** > **All**.
2. Select the project for risk assessment.
   Ensure that risks for this project are present. See Add risks for a project.
3. Click the Risks related list.
4. Select the risk you want to assess.
5. Click **Assess Risk**.
   The values are shown based on the integration configuration.
6. In the **Approver** field, select an assessor for the project risk.
7. Click **Submit**.

### Result
The risk moves to the risk assessor's workflow.

Related topics

Configure Project Portfolio Management and Advanced Risk integration

#### Assess project risks using Advanced Risk Assessment

Assess the project risks by responding to predefined factors or questions. Arrive at a risk score for the project.

### Before you begin
Role required: it_project_manager and sn_grc.business_user

### About this task
A risk is assessed for inherent risks and residual risks. An inherent risk is a risk that has no mitigating controls. A residual risk is a risk that remains after the controls are accounted for. The workflow of the risk assessment is determined by the risk admin on the risk assessment methodology configurations. If the project manager wants to enable approval of the assessment, then the project manager can configure the approval flow in the Project Integration Configuration form. If an assessment for a risk has been taken before, the results of the previous assessments appear in the Previous Assessments related list.
A risk assessor can do the following:

- Assess the risks that were added for a project.
- Decide if the risks must be elevated to enterprise risks.

To understand how to assess risks on a risk assessment instance and how to respond to the questions, refer to Understanding the risk assessment instance.

### Procedure
1. Navigate to **All** > **My Tasks** > **Module**.
2. Select the assessment that you want to assess.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click **Assess**.
4. In the Inherent Assessment section, respond to the factors as appropriate and click **Save and Calculate**.
5. In the Results section, you can override the computed score.
   a. If you think that the computed risk score is not correct, select the **Override computed score** check box to override the computed risk score.
   b. In the **Override inherent risk** field, select a value to override the computed risk rating. This field appears only when the **Override computed score** option is selected.
   c. In the **Comments** field, enter your justification for overriding the computed risk rating.
6. Click **Perform residual assessment**.
   a. In the Residual Assessment section, respond to the factors as appropriate.
   b. Click **Save and Calculate**.
7. Click **Mark as complete**.
8. Click **Request Approval**.
   The option to request approval appears only when the Project Integration Configurations form has the approvers identified. In that case, the workflow moves to the Awaiting Approval state. But if the option to request approval is not selected, then the workflow moves to the Monitor state.

### What to do next
Elevate a project risk to enterprise risk.

#### Elevate a project risk to enterprise risk

Elevate a project risk to an enterprise risk if the project risk has an impact on the enterprise.

### Before you begin
Role required: it_project_manager or sn_grc.business_user

### About this task
If you find that a project risk has an impact on the enterprise, then you can elevate the project risk to an enterprise risk. After a risk is elevated, the project risk is automatically copied to the enterprise risk register. An elevated risk needs an assessment on the enterprise impact. The enterprise risk is always connected to the project risk. If a project risk is retired, then the enterprise risk also gets retired.

### Procedure
1. Navigate to **All** > **Project** > **Projects** > **All**.
2. Select the project for risk assessment.
3. Select the assessed risk that you want to elevate.
4. In the related links, click **Elevate to Enterprise Risk**.

> **Note:** The assessor is predefined in the **Assessor** field. The value in this field is obtained from the Project Integration Configuration form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. In the **Approver** field, select an approver.
6. Click **Submit**.

### Result
A new risk assessment is generated for enterprise risk assessment. The assessment is sent to the enterprise risk assessor.

### What to do next
Based on the assessors identified as the enterprise assessors in the Project Integration Configuration form, the enterprise risk manager gets a notification to assess the risk from an enterprise risk perspective. The steps to perform the risk assessment are the same as given in Assess project risks using Advanced Risk Assessment.

## Application risk assessment using Advanced Risk Assessment

Manage digital risks of business applications easily by integrating GRC with business applications. By integrating, you get real-time insights into the digital risk posture of business applications, have improved communication between application owners and IT risk managers, and can reduce workloads.

Enterprises use Application Portfolio Management (APM) to manage their inventory of business applications. Examples of business applications are Zoom, Workday, Jobvite, and so on. Each business application has two owners:

- IT Application owner: Owns the application from the IT team and is the primary point of contact. The IT application owner is also known as the application product owner or application owner.
- Business owner: Owns the application for its business uses. The business owner is the executive sponsor of the business application. The owner is generally from the business who sponsors the application. For example, finance applications are usually sponsored by the head of finance.

When you integrate GRC with APM, you can simplify the work of IT risk managers by identifying the risks and the necessary controls. You can mitigate the digital risks of business applications. You can also ensure that the controls are effective. The benefits of this integration are the following:

- Reduces the time spent by risk managers and by the application owners of digital risks.
- Provides faster and more efficient communication between the application owners and risk managers.
- Provides an overview of the digital risk posture of business applications.
- Enables continuous monitoring of the applications.

The users who benefit from this integration are shown in the following figure:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Beneficiaries of APM and Risk integration**

## Key Personas



**IT Risk Manager**
- Primary person responsible for application risk
- Decides the Business Impact Analysis (BIA) rating for the application
- Identifies and implements the necessary controls for the application



**IT Application Owner / Product Owner**
- Maintains the business application and is primary point of contact
- Provides accurate information about the application for:
  - Risk and control identification
  - Business impact computation
- Assists IT Risk manager in implementation of controls



**Application Sponsor / Business Owner**
- Business sponsor accountable for the application
- Monitors the application status on a periodic basic



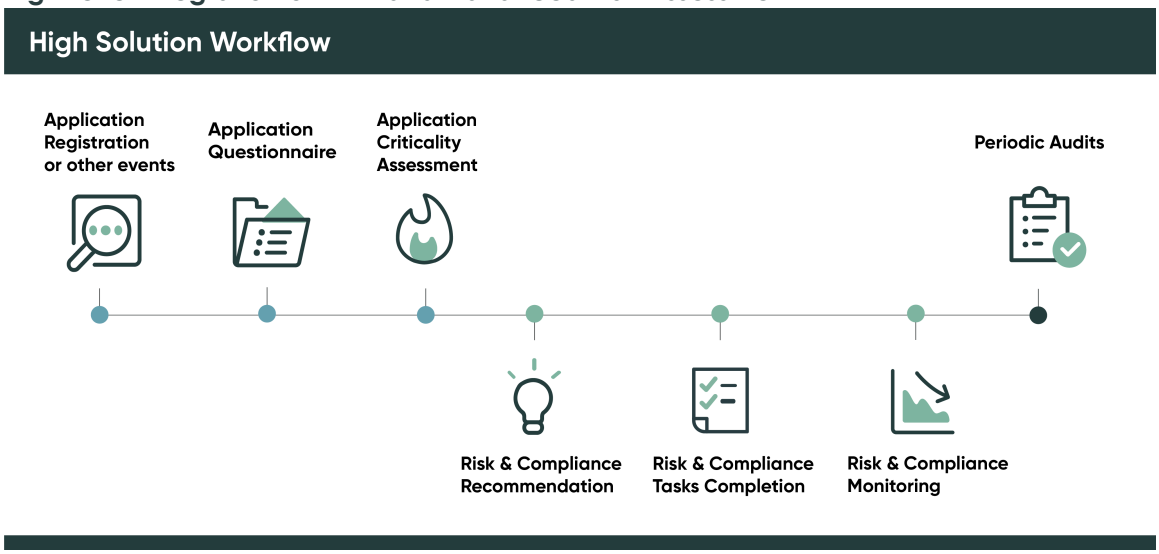
**IT Governance Team**
- People from compliance and audit team acting as a 2nd and 3rd line of defense
- Conduct audits of the business application to ensure compliance
- Create IT Governance framework that all business applications should comply with

The Application Risk Assessment feature is available when you activate the Advanced Risk plugin. But the default configurations for the APM risk identification record are available only when you have the APM integration with Risk Management plugin (com.snc.apm_risk_assessment) enabled.

The following image shows the high-level workflow of the integration:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**High-level integration of APM and Advanced Risk Assessment**




Related topics

Workflow of risk identification for business applications

### Workflow of risk identification for business applications

When assessing an application for risks, the application goes through various stages of risk identification and assessment. You can define the identification and assessment workflow based on your requirements.

Before the risks of an application are assessed, the application must be created in the Business application table and brought to GRC. After the application comes to GRC, a risk identification record is created. The application owner provides information about the application to the IT Risk Manager. The IT Risk Manager then maps the recommended risks, citations, and policies.

Consider the following example to understand the workflow of risk identification and assessment for a business application. A new business application is introduced into your organization. This new application is a part of the Business Application table. The new application has two owners:

- IT application owner
- Business owner: This user must have the sn_grc.business_user role.

**Note:** Your organization can use different roles.

At this point, the application is not a part of GRC. It must be brought to GRC as an entity before its risks can be assessed. The new application must also have information objects associated with it.

The workflow and approvers of the application risk assessment are determined by the settings in the Risk Identification Configuration form. Refer to Set up risk identification integration to understand the process of defining the workflow. To reinitiate risk identification, a flow designer action is provided.

When assessing a new business application, the workflow of the risk identification is as follows:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. A business application is created either automatically or by an application owner in the business application table.
2. GRC detects the new business application. A GRC entity is created for the new application. The detection is handled by the GRC Profile Generation scheduled job that runs in the background.
3. A new risk identification record is created for the application.

   **Note:** The Risk Manager can modify the configuration record and determine the workflow of the assessment. After a risk identification configuration is published, the risk manager can modify only some fields in the configuration record.

4. A questionnaire is initiated and sent to the application owner to collect details about the application.
5. The application owner responds to the questionnaire.
6. The IT Risk Manager reviews the responses. If the responses are unsatisfactory, the manager sends the questionnaire back to the application owner.

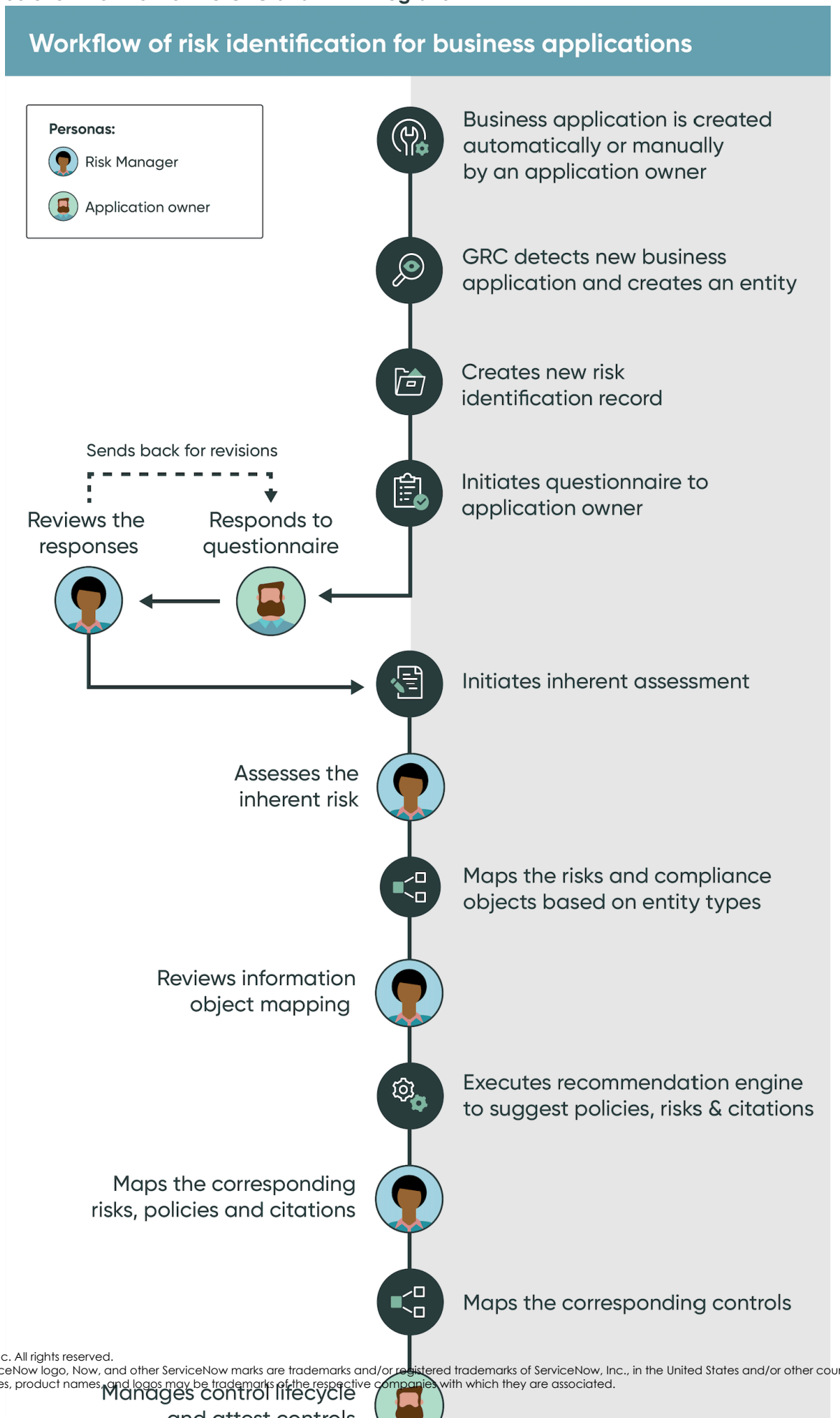
   **Note:** If the questionnaire is sent back, then the new responses are reverted to their original form.

7. Based on the configuration, after the IT Risk Manager is satisfied with the responses, the system initiates the inherent assessment.
8. GRC maps the risks and compliance objects based on the entity types.
9. The IT Risk Manager reviews the information object mapping.
10. The system executes the recommendation engine based on the algorithm selected in the configuration.
11. The IT Risk Manager reviews and maps the recommended risks, policies, and citations based on the associated information objects.
12. The IT Risk Manager maps the recommended controls based on associated citations, policies, and risks.
13. The application owner manages the control life cycle and attests the controls.

The following figure represents the workflow of the solution.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Solution workflow of the GRC and APM integration




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## States of the risk identification record

After the risk identification configuration moves to the Published state, a risk identification record gets created for the related entity.

The risk identification record moves through the following states:

- New: A new record is created
- Information Gathering: The information about the application is collected.
- Review: The Risk Manager reviews the information.
- Inherent Assessment: The Risk Manager performs inherent risk assessment.
- Risk Mapping: The Risk Manager maps the necessary risks, citations, and policies.
- Monitor: The risks are monitored.
- Retired: The risks are retired as necessary.

After the risk identification configuration moves to the Retired state, the configuration becomes invalid and risk identification records are not created for related entities.

In terms of its life cycle, a risk identification record goes through the following states:

1. New
2. Information Gathering
3. Review
4. Inherent Assessment
5. Risk Mapping
6. Monitor
7. Retired

### Set up risk identification integration

Before assessing an application, specify the target application where the risk identification must be initiated.

#### Before you begin

Make sure you have the following applications:

- Application Portfolio Management must be installed if you want the recommendation engine enabled and want to use the integration.
- Application Portfolio Management integration with Risk Management (com.snc.apm_risk_assessment) must be installed. This application is required only if you want to use the integration.

Role required: sn_risk.admin

#### About this task

The Risk Identification Configuration form contains an entity type and a default identification record for the business application table. As a risk admin, you can either modify the default record or create your own configuration. The steps in this procedure are for creating a record. The Risk Identification Configuration form is used to do the following:

- Gather information about the application by using a questionnaire.
- Determine the criticality of the application.
- Determine if an inherent assessment for the application is required.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Identify risks and map the relevant controls.
- Choose to receive recommendations for risks and controls.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Risk Identification Configuration**.
2. Select **New**.
3. On the form, fill in the fields.

**Risk Identification Configuration form**

| Field | Description |
|---|---|
| Name | Name of the configuration. An example is `Risk Identification for Business Application`. |
| Configuration level | The level where the configuration is done. The choices are as follows:<br>◦ Entity class<br>◦ Table |
| Target entity class | Entity class for which the risk identification questionnaire is initiated. For each entity of this entity class, a risk identification record is automatically created. This field appears only when **Entity class** is selected from **Configuration level**. |
| Target table | Table that contains the application record. For each entity of this table, a risk identification record is automatically created. This field appears only when **Table** is selected from **Configuration level**. |
| State | State of the configuration. This field is automatically set to **Draft**. |
| Risk manager group | Group which reviews the risk identification workflow. The users who belong to this group must have the sn_risk.manager and sn_compliance.manager roles. |
| Identification questionnaire | Option to initiate a questionnaire for gathering information about the application. |
| Inherent assessment | Option to perform inherent assessment or business impact analysis (BIA) assessment. |
| Recommendation engine | Option to recommend risks and controls. This option is available only when the **Target table** field has **Business Application**. |
| Identification Questionnaire | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Questionnaire | Questionnaire used for information gathering. |
| Respondent type | Respondent of the questionnaire. The choices are as follows:<br>◦ Entity owner<br>◦ User on target record |
| Questionnaire review required. | Option to require that the questionnaire is reviewed by a reviewer. |
| Respondent field | Field on the target table that contains the respondent for the questionnaire. This field appears when the **Respondent type** field has **User on target record**. |
| Inherent Assessment | |
| Review for inherent assessment required | Option to choose if the inherent assessment must be reviewed. |
| Risk assessment methodology | Option to select the risk assessment methodology (RAM) to perform inherent assessment. You can see the list of RAMs associated with the selected Target table.<br>**Note:** Only published object-based RAMs with the inherent assessment option enabled are available for selection. |
| Approver type | Type of approver for the inherent assessment. The choices are as follows:<br>◦ User on target record<br>◦ Group<br>**Note:** This field appears only when **Review for inherent assessment required** option is selected. |
| Approver | Approver for the inherent assessment. For a business application, the approver is the business owner of the application.<br>**Note:** This field appears only when **User on target record** is selected from **Approver type**. |
| Approver group | Approver group for inherent assessment. This field appears only when the **Approver type** field has **Group**.<br>**Note:** This field appears only when **Group** is selected from **Approver type**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Recommendation Engine | |
| The Recommendation Engine section appears only when the **Target table** field has **Business Application**. | |
| Recommendation engine algorithm | Specify the recommendation engine. The choices are as follows:<br>◦ None<br>◦ Based on information object mapping<br>For details on information objects, see Information objects. |
| Frequency | |
| Frequency | Frequency of the reinitiation of the workflow.<br>**Note:** The next run date of the reinitiation of the workflow is calculated based on the frequency defined in the risk integration configuration record. This frequency ensures continuous evaluation of the application. |
| Month | Month when the job must run. |
| Day of month | Day of the month when the job must run. |

4. Select **Submit**.
5. To define the RAM mapping for the risk identification configuration, do the following actions:

   a. In the Risk Identification Configuration to RAM Mappings section, select **New**.
   The Risk Identification Configuration to RAM Mappings section appears only when **Entity class** is selected from **Configuration level**.

   b. On the form, fill in the fields.

**Risk Identification Configuration to RAM Mapping form**

| Field | Description |
|---|---|
| Risk identification configuration | Risk identification configuration for the RAM mapping. This field is automatically set to Risk identification configuration number. |
| Table | Table on which you want to define the RAM mapping. |
| Risk assessment methodology | Option to select the RAM to perform inherent assessment. You can see the list of RAMs associated with the selected table. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** Only published object-based RAMs with the inherent assessment option enabled are available for selection. |

c. Select **Submit**.

6. Select **Publish** to publish the record.

Related topics

Workflow of risk identification for business applications

### Respond to an application questionnaire

Respond to a questionnaire about an application for risk assessment.

#### Before you begin
Role required: none.

#### About this task
The Risk Identification form contains multiple stages for the workflow. When an application is created in GRC as an entity, a questionnaire is sent to the IT application owner. The questionnaire is useful for risk managers to identify threats and mitigating controls.

#### Procedure
1. Navigate to **All** > **Self-Service** > **My Assessments & Surveys**.
   Alternatively, you can also navigate to **My Risk Identification Questionnaires** to access the questionnaire.
2. Open the record with the assessment that you must respond to.
3. Enter your responses.
4. Click **Submit**.

#### Result
The state of the risk identification record moves from the Information Gathering state to the Review state.

#### What to do next
The IT Risk Manager can review the responses and can either send the questionnaire back or accept the responses.

### Review responses and perform inherent risk assessment

Compute the overall risk score for an application by performing an advanced risk assessment. After the IT application owner responds to the questionnaire, a risk manager reviews the responses and performs the inherent assessment.

#### Before you begin
Role required: sn_risk.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

After the risk assessor returns the assessment questionnaire, you can review the questionnaire as the risk manager. Based on your review, you can initiate a risk assessment for the application.
The risk assessment task is initiated to the group responsible for performing the assessment. The task is available in **My Group Tasks**. Any risk manager who is a part of the group can perform the assessment. The assessors usually don't vary.

You can choose to use either the manual factors or the automated factors. By default, there are three manual factors which are associated to a risk assessment methodology. There are also three automated factors which are not associated to any risk assessment methodology. The names of the factors are:

- Confidentiality Impact
- Integrity Impact
- Availability Impact

Some of the factors or questions on the risk assessment instance might already have an answer or a response. These values are derived from the responses of the application owner. You can view how the value was calculated.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Risk Identification** > **All**.
2. Open the record with the assessment that you must review.
3. In the Questionnaires related list, click **View responses** for the required assessment.

   a. If you are not satisfied with the responses provided in the questionnaire, click **Reject Questionnaire**.
   The respondent receives an email and is asked to resubmit the questionnaire.

   b. If you're satisfied with the responses provided by the application owner, then perform the inherent assessment by clicking **Perform Inherent Assessment**.
   The risk assessment instance link is created.

   To understand the risk assessment process and how to respond to questions, refer to Understanding the risk assessment instance.
4. Click the risk assessment instance link that is generated.
5. Respond to the questions or manual factors.
6. Right-click and save the form.
7. Click **Request Approval**.

### Result

The approver selected in the Risk Identification Configuration form can review the inherent assessment. The state on the Risk Identification form is moved to the Risk Mapping state.

### What to do next

Associate risks, citations, policies, and controls with a risk identification record.

#### Associate risks, citations, policies, and controls with a risk identification record

After the inherent assessment is completed, you can associate risks, citations, policies, and controls with the risk identification record. You can identify what methods to use to mitigate the risks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_risk.manager and sn_compliance.manager

### About this task
Risks, citations, and policies can be associated manually or by using the recommendation engine. The recommendation engine provides automatic suggestions for risk, citations, and policies. The choice to enable the recommendation engine is made in the risk identification configuration record. The choice is available only for the business application table. For the recommendations to be enabled, the risks statements, citations, and policies must have information objects.

### Procedure
1. Navigate to **All** > **Advanced Risk Assessment** > **Risk Identification** > **All**.
2. Open the record for which you want to associate risks, citations, and policies.
   This is the record for which you performed the inherent assessments.
3. Click **Associate Risks**.
   The Information Objects Mapping related list and the Risks related list appear. At this stage, you can either manually add risks or allow the recommendation engine to recommend risks.
4. To add risks manually, click **Add from library**.
5. To use the recommendation engine, do the following:
   a. Click **Recommend Risks** to use the recommendation engine.
   b. Select the appropriate risk statement and click **Add Risks**.
6. To add citations and policies, click **Associate Citations and Policies**.
   The Citations related list and Policies related list appear.
7. Add the required citations and policies either manually from the library or by using the recommended policies and citations.
8. To associate controls, click **Associate Controls**.
9. Add the required controls either manually from the library or by clicking **Recommended Controls**.
   The controls are created based on the control objectives.
10. To move a control to the Attest state, select the control and click **Initiate Attestation**.
11. Click **Monitor** to move the record to Monitor state.

Related topics

Recommendation engine for risk and compliance mapping

#### Recommendation engine for risk and compliance mapping

A recommendation engine is a system that suggests products, services, and information to users based on data analysis. A recommendation engine boosts revenues and other essential metrics.

Recommendations derive from various factors, such as the history of the user and the behavior of similar users. An example of a recommendation engine is a video-sharing website. Based on your viewing history and preferences, the website recommends videos. Some recommendation engines are rule-based. Risk and compliance mapping in GRC uses a rule-based recommendation engine.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When using the recommendation engine, the risk manager has to map the information objects with their risk statements, citations, and policies. The key features of the recommendation engine are the following:

- Uses the concept of information objects to recommend the risks and compliances.
- Matches the business applications with the risk and compliance libraries by comparing the information objects of the libraries.
- Allows IT risk managers to define and map risk and compliance libraries based on the information that is contained within the application.
- Reduces the time spent on mapping the risk and compliance libraries.
- Improves the overall time it takes to scope the right applications and assets that must be audited for a particular type of audit.

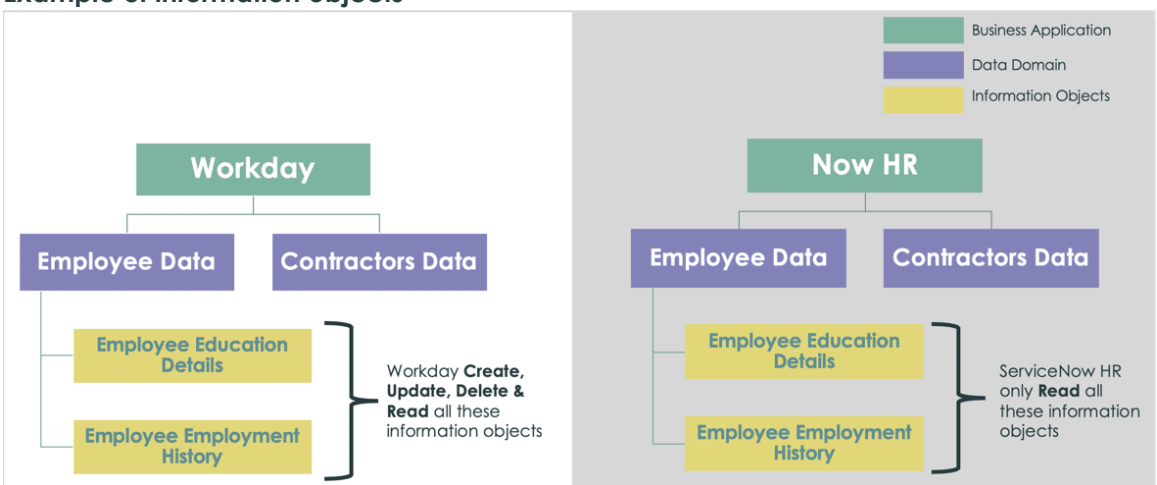
### Information objects

Information objects are a part of the information portfolio management capability in the Application Portfolio Management application.

An information object is a configuration item that displays information in an organized form. The purpose of the information object is to logically describe the type of data that is exchanged between the application and the database. After information objects are created, they are mapped to business applications. For a given business application, the information objects determine if information can be created, updated, deleted, or read in that business application. This ability allows application owners to efficiently manage information. From an information security management perspective, this ability enables the risk and compliance function to define the right level of controls that must be applied.

The following figure shows an example of information objects. There are two applications: Workday and Now HR. Both applications store employee information. Employee information is an information object. The Now HR application can only read employee information, while the Workday application has more permissions. The risks and controls that apply to the applications are similar. However, Workday not only reads, but also creates, updates, and deletes the employee information. This means that the risks associated with Workday are higher, and so the controls applied to Workday are more stringent.

**Example of information objects**




## Integration of advanced risk assessment with other applications

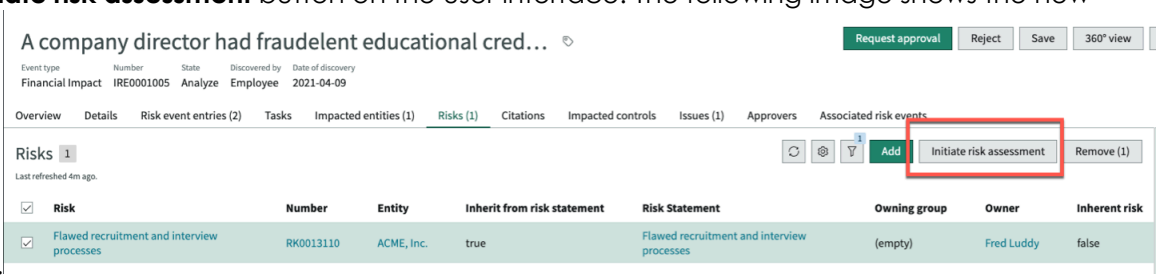
As an administrator, you can embed risk assessments within other workflows and define rules for when risk assessments must be initiated. The key benefit of embedding risk assessments

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

is the digitization of the workflow so that assessments are initiated automatically without manual effort.

Prior to the San Diego release, you could perform risk assessments in a cyclic manner. This means that earlier risk assessments were performed only few times in a year and thus your risk posture reporting might not be accurate. To address this issue, you can now perform event-driven risk assessments. Event-driven risk assessments mean that when an event occurs, you can perform a risk assessment. Performing event-driven risk assessments help you to get a quick view of the actual risk posture and take the necessary corrective actions. You can integrate advanced risk assessment with any application and perform risk-based assessments in your workspaces. By default, ServiceNow® provides the integration of advanced risk assessment with risk events in the Risk Workspace.

To integrate risk assessment in an application in your workspace, you must perform the configuration steps given in the Risk assessment integration in workspace [KB0999135] article in the Now Support Knowledge Base. After you perform the configuration steps, you can see the **Initiate risk assessment** button on the user interface. The following image shows the new button.




Although you can integrate the Initiate risk assessment feature on any application in your workspace, this article uses risk events as an example. When you analyze a risk event and identify the relevant risks, you can easily initiate risk assessments for those risks by integrating the advanced risk assessment workflow in your risk events. This integration enables you to perform risk assessments without going through the entire process of creating risk assessment scopes. Prior to the San Diego release, for a risk assessor to perform a risk assessment, the risk user was required to create a risk assessment scope defining the entity, the assessor, and the approver.

When you initiate an assessment for a risk that is created for a risk event, although the risk assessment methodology (RAM) is set to the primary RAM of the entity class, you can select a different relevant risk assessment methodology. Only those risk assessment methodologies that are associated with the entity class of the selected risk are available for selection. You can then specify the assessor and approver for the risk assessment. Only users with the sn_risk_advanced.ara_assessor role can be the assessors and users with the sn_risk_advanced.ara_approver role can be the approvers. For more information on these roles, see Roles for performing advanced risk assessment. Earlier, the approvers were defined when the risk administrators created the risk assessment scopes. However, when you initiate a risk assessment from an application, you can specify the approvers at the time creating the assessment. You cannot change the approvers once you have specified them. If the approver is set as **Same as assessor's manager**, then the approver is automatically set depending on the assessor. You can also define the number of days after which the assessment will be considered overdue.

Even when you initiate a risk assessment from an application using the API, you can add those risks to the risk assessment scope at any time. After the risk is added to the risk assessment scope, the frequency of the assessment is based on the frequency defined in the risk assessment scope.

There could be some scenarios when you maybe unable to initiate a risk assessment from an application. Those scenarios are listed as follows.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- If you select multiple risks and try to initiate the assessments at once. The reason for this is that different risks can have different entities and can have different risk assessment methodologies.
- If an in-progress risk assessment exists.
- If a risk assessment methodology is not defined for the entity for which the risk exists.

## Integration of Employee Center and GRC

The integration of GRC tasks with the Employee Center makes it easier for employees to complete the GRC tasks easily and effectively. This integration allows them to report risk events or request policy exceptions and makes GRC more useful in the organization.

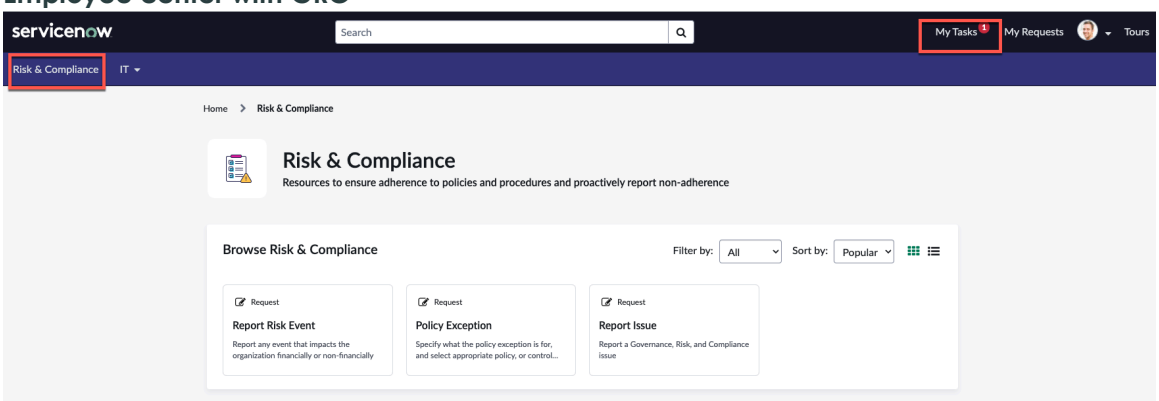
The Employee Center portal is a unified portal that helps connect systems across the enterprise to one destination site that provides a simple and centralized experience for employees with easy to configure options. To learn more about the Employee Center, refer to Exploring Employee Center.

If you integrate GRC with the Employee Center, you can provide all employees an interface to perform the following tasks:

- Quickly report risk events.
- Report an issue.
- Request a policy exception.
- Use **My tasks** to get a consolidated view of all your tasks and perform them immediately.
- Respond to a risk identification questionnaire.
- Complete other GRC tasks such as control attestation questionnaire, classic risk assessments and so on.

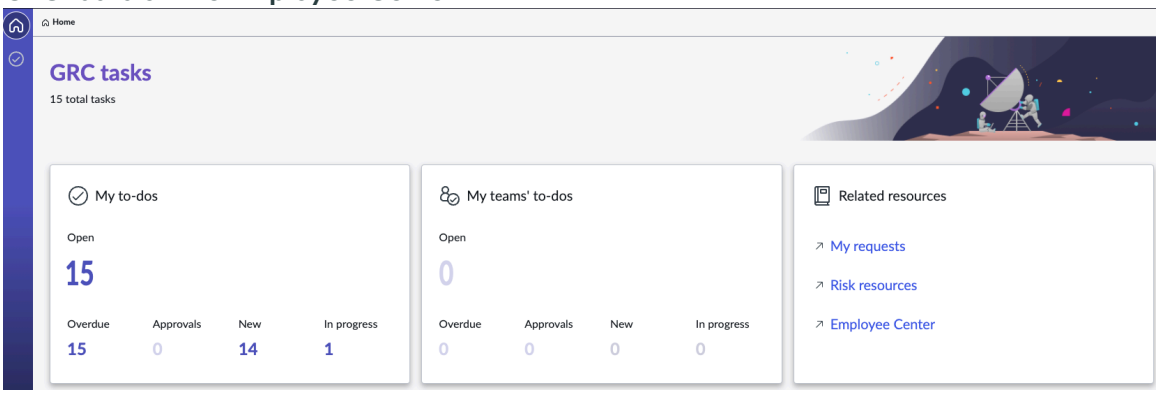
The following images show you the user interface of the Employee Center.

### Employee center with GRC




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### GRC tasks on the Employee Center




## Manage continuous monitoring for risks between Risk Management and Vulnerability Response

Continuous monitoring for risks is a feature integration between the GRC: Risk Management and the Security Operations Vulnerability Response products, which uses indicators to quickly identify high impact vulnerabilities based on business impact.

Risk administrators, managers, or users can monitor critical vulnerabilities by viewing the direct effect on risk posture. A new **Business Services** entity type and indicator templates automatically identify impacted services that are critical, represent a loss of availability, and are greater than two weeks old. These high-risk vulnerabilities can result in a breach and possible loss of intellectual property.

**Note:** The Entity type called 'Critical Business Services' is set to inactive by default and must be turned on.

### Continuous monitoring for risk workflow

1. The system admin activates the Risk Management and Vulnerability Response plugins.
2. The risk administrator creates risk statements and indicator templates.
3. The risk manager associates the **Critical Business Services** entity type to the risk statements and indicator templates.
4. The Vulnerability Response application ingests vulnerability data from scanners related to impacted services.
5. As risks are identified, issues are generated and assigned to the appropriate business service owners.
6. Dashboards provide an up-to-date view for business stakeholders as risks are identified and remediated.

## Integrating Microsoft 365 with Management Reporting of Risk

The Management Reporting of Risk (sn_grc_mgmt_report) integration provides reporting capabilities to Risk reporting managers to report ServiceNow Risk Management system data, list reports, charts, pivot, and multi-pivot reports using Microsoft Word.

The risk managers prepare reports for board members or senior management periodically to provide updates on the risk profile based on the information available in ServiceNow.

This integration enables the risk reporting managers to view the inventory of the ServiceNow Risk Management data links on the report and refresh the inserted data to be in synchronization with the latest ServiceNow Risk Management data. An audit trail is also established between the data imported and the ServiceNow instance. The audit trail

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

provides any auditor the ability to select the links in the document and access the source of the data in the ServiceNow instance.

**Note:** This integration is compatible with the desktop version 16.71 (23031200) and the web version 16.0.16412.41005 of Microsoft Word. However, the charts aren't interactive in the web version. This means that you can't modify the chart colors, formats, and so on. The supported Windows Office version is 2303 (Build 16130.20394).

You can also change the format, style, and colors of the imported data. The following chart styles are supported:

**Supported chart styles**

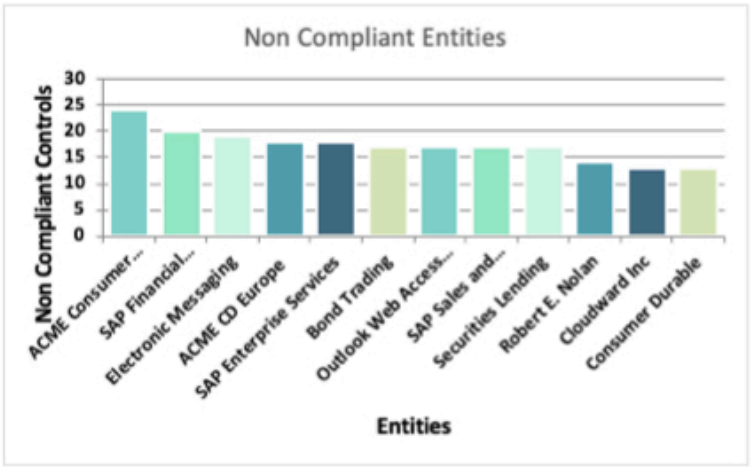
| Chart type | Styles supported |
|---|---|
| Pie chart | • Chart color<br>• Display data label<br>• Chart title<br>• Show legend |
| Bar chart | • Chart color<br>• Display data label<br>• Chart title<br>• X-Axis and Y-Axis<br>◦ Title<br>◦ Title bold<br>◦ Display grid<br>◦ Label bold |
| Horizontal bar chart | • Chart color<br>• Display data label<br>• Chart title<br>• X-Axis<br>◦ Title<br>◦ Title bold<br>◦ Display grid<br>◦ Label bold<br>• Y-Axis<br>◦ Display grid<br>◦ Label bold |

The following image shows how the imported data appears in a document.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### How various types of imported data appears in a document

The data that is imported from an instance into a Word document.







| Control | Classification | Control effectiveness | Design effectiveness | Operating effectiveness | Actual start | Status |
|---|---|---|---|---|---|---|
| Establish and maintain electronic storage media management procedures. | Preventive | Ineffective | Effective | Ineffective | 2027-07-02 22:17:48 | Green |
| Manage changes. | Preventive | Ineffective | Ineffective | None | 2023-10-23 08:15:01 | Green |

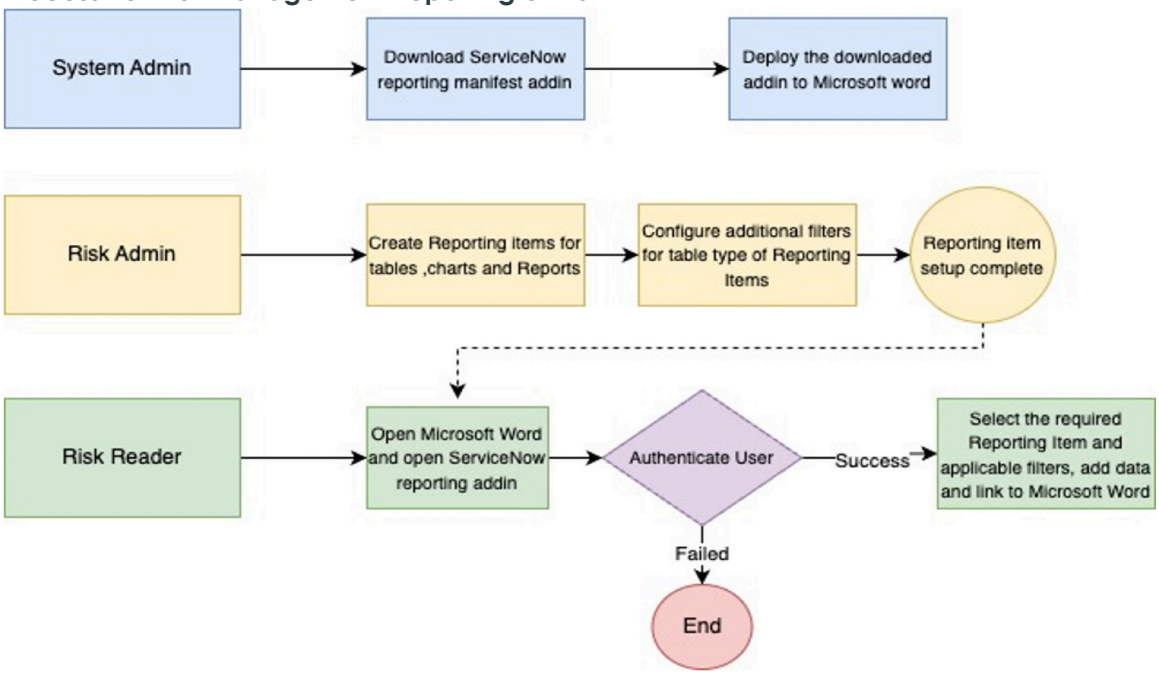
### Workflow of Management Reporting of Risk

The Management Reporting of Risk integration utilizes a workflow that requires participation from multiple user roles such as system administrators, Risk administrators, and Risk managers. By defining a clear workflow, individuals and teams can better understand their roles and responsibilities and generate the necessary reports.

The following figure displays the complete workflow of using the Management Reporting of Risk integration to generate reports in a Microsoft Word document.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Process flow for Management Reporting of Risk




To generate Microsoft Word reports:

1. Download the ServiceNow Reporting add-in: As a system administrator, download and install the Risk manifest file. A manifest file contains information about the files included in a software application or package. It's used by the software installer to ensure that all the necessary files are installed in the correct locations. At this stage, you must also work with your Microsoft 365 administrator to upload the manifest file to the Microsoft Word application. The Microsoft 365 administrator has the necessary access rights.
2. As a Risk administrator, set up the Microsoft 365 reporting configuration records to specify which tables, reports, and charts from your ServiceNow® instance must be used to import data into your Microsoft Word. You can also specify the columns from a table from which you want to import data.
3. As a Risk administrator, you can configure additional reporting filters. These filters specify at a granular level what data must be imported to the disclosure report from a table.
4. As a Risk manager, go to your Microsoft Word document, authenticate yourself with the ServiceNow® credentials, and import the data from your instance to the document. You can alter the formatting of the data according to your preferences.

### Install the ServiceNow Reporting add-in for risk reporting

Install the ServiceNow Reporting add-in to your Microsoft Word document. This add-in is required to import reports and data from your ServiceNow® instance to Microsoft Word documents to create risk reports.

#### Before you begin

Ensure that the following plugins are activated:

- sn_esg_msoff_intg
- sn_outlook_addin
- sn_grc_mgmt_report

Role required: sys_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **ServiceNow Add-Ins for Office** > **Office Add-In Manifests**.
2. From the Office Manifests list, select **ServiceNow Reporting**.
3. Select **Download Manifest**.
4. To enable the add-in, contact your Microsoft 365 account manager who can use the manifest file you downloaded in step 3.

### What to do next

For detailed instructions on how to deploy the manifest file, see the Deploy add-ins in the Microsoft 365 admin center [KB1307378] article in the Now Support knowledge base.

To configure the HTTP response headers for the add-in for Microsoft Word in the browser, see the Response header resolution [KB1434453] article in the Now Support knowledge base.

## Set up Microsoft 365 reporting configuration in risk

Set up the Microsoft 365 reporting configuration records to specify the data points and reports that you want to import in to a Microsoft Word document for risk reporting purposes.

### Before you begin

Role required: sn_risk_advanced.ara_admin

### About this task

Data is imported into a Microsoft Word document for risk reporting purposes. You must specify which tables and reports from your ServiceNow instance must be used to import data into the Microsoft Word. You can also specify the columns from a table from which you want to import data. Only those reports that are either created by or shared with the Risk administrator are available for selection.

### Procedure

1. Navigate to **All** > **Management Reporting of Risk** > **Microsoft 365 Reporting Integration** > **Reporting Configurations**.
2. From the Microsoft 365 reporting configurations list, select **New**.
3. On the Microsoft 365 reporting configuration form, fill in the fields.

#### Microsoft 365 reporting configuration form

| Field | Description |
|---|---|
| Business domain | Domain from where the configuration is created. This field is automatically set to **Risk**. |
| Reporting item | Name of the configuration. For example, if you want to get data about your Risk statement in your word document, you can provide a name such as `Risk statement`. |
| Source type | Source from which you want to fetch the data. The choices are as follows:<br>◦ **Table**: Select this option when you want to import data from a table.<br>◦ **Report**: Select this option if you want to import data from a predefined report or |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | chart. For more information on how to create a report, see Create a report with Analytics Q&A.<br><br>**Note:** Only list reports, pivot reports, multi-level pivot reports, horizontal and vertical bar charts, and pie charts are available for selection. Stacked bar charts and grouped bar charts aren't supported. |
| Source table | Source table to fetch data from. This field only appears when **Table** is selected from the **Source type** field. |
| Filter | Filter conditions to filter the records. This field only appears when **Table** is selected from the **Source type** field. |
| Columns | Column from the table whose values are to be inserted. This field only appears when **Table** is selected from the **Source type** field. |
| Source report | Available report to be inserted in the disclosure report. This field only appears when **Report** is selected from the **Source type** field. |
| Active | Option to indicate if the record is active. Only active records are available for selection in the document. |

4. Select **Submit**.

### What to do next
Add additional reporting configuration filters to the reporting configuration. These filters help to fetch the data into your Microsoft Word disclosure report. For more information, see Add additional reporting configuration filters for a Microsoft 365 configuration record in risk.

#### Configure a business domain role in Management Reporting of Risk

Configure the business domain roles so that users of a particular domain can select the domain for which they want to import the data. Only those users who are added during the configuration are able to view the domain on the Microsoft Word document.

### Before you begin
Role required: sn_risk_advanced.ara_admin

### Procedure
1. Navigate to **All** > **Management Reporting of Risk** > **Microsoft 365 Reporting Integration** > **Business Domains**.
2. Select the default Risk domain name record.
3. Select the **Roles** field.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Add or remove the roles as required.
5. Select **Update**.

### Add additional reporting configuration filters for a Microsoft 365 configuration record in risk

Add additional reporting filters to specify at a granular level what data must be imported to the report from a table using the Management Reporting of Risk application.

#### Before you begin
Role required: sn_risk_advanced.ara_admin

#### About this task
When you specify that you want to import data from a particular table, you must also specify from which exact record of the table you need the data. For example, assume that you specify that you want to fetch data from the sn_risk_risk table. This table may have multiple records. Therefore, you must specify the exact record from which you want to fetch the data. You can specify as many filters as you require.

#### Procedure
1. Navigate to **All** > **Management Reporting of Risk** > **Microsoft 365 Reporting Integration** > **Reporting Configurations**.
2. Open the record for which you want to add the additional reporting configuration filters.
3. On the Microsoft 365 reporting configuration filters related list, select **New**.
4. On the form, fill in the fields.

**Microsoft 365 reporting configurations filter form**

| Field | Description |
|---|---|
| Reporting configuration | Name of the configuration to which you're adding additional filters. This field is automatically set. |
| Field name | Name of the field from which data must be fetched. For example, for the risks table, you can specify the **Name** field. If you select a name, then all the names of the risks are available for selection during data import. |
| Order | Order of the field as it would appear on the add-in pane of the document. |
| Aggregate on time dimension | Option to aggregate the report configuration source table data based on the chosen time dimension. For more information about this option, see the example in the procedure. This field only appears when the **Field name** has **Time dimension**. |
| Time dimension | Time dimension for which data must be aggregated. The list of time dimensions are:<br>◦ Year<br>◦ Semi-annual |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Quarter<br>◦ Month<br>◦ Week<br>◦ Date<br>Select the dimensions according to your requirement and move them from the Available list to the Selected list.<br>**Note:** This field only appears when the **Aggregate on time dimension** option is selected. |

5. Select **Submit**.

### Result
The configuration data is ready to be imported in to your add-in.

#### Add the ServiceNow Reporting add-in into Microsoft Word

Before you can import data into your Microsoft Word document to create your disclosure reports, you must add the ServiceNow Reporting add-in to your Microsoft Word.

### Before you begin
Role required: Any user of the Microsoft Word document.

### Procedure
1. Open the Microsoft Word application.
2. On the menu bar, select **Insert**.
3. Select **Add-ins**.
4. Select **ADMIN MANAGED**.
5. Select the **ServiceNow Reporting** add-in.
6. Select **Add**.

### Result
The Microsoft 365 for ServiceNow Reporting integration is activated and the following buttons are available on the Microsoft Word document in the **ServiceNow Reporting** add-in.

- **Insert Link**
- **Manage Links**

#### Import risk data in to a Microsoft Word

Import and insert data such as Risk data points and reports into a Microsoft Word report document from a ServiceNow instance. You can only import and insert the data that is configured in your reporting configurations.

### Before you begin
Role required: sn_risk_advanced.ara_reader

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to the Microsoft Word document in which you want to insert data.
2. On the ribbon, select **Insert Link**.
   On the right side pane, the ServiceNow login screen appears.
3. To log in to your ServiceNow instance, select **Log in**.
   a. A message is displayed that states that ServiceNow Reporting will display in a new window, select **Allow**.
   b. On the ServiceNow login screen, provide your credentials.
   c. Select **Allow**.
4. To insert a Risk data point from a table into the document, move the cursor at the point where you want to insert data.
   a. Select the **Data** tab on the right side pane.
   b. The **Business domain** field is set to **Risk**.
   c. In the **Reporting Item** field, select the reporting configuration you want to insert.
      The additional filters dynamically appear based on the configuration record selected.
   d. In the **Name** field, select the name of the configuration record.
   e. In the **Value to insert** field, select the column from which you want to insert data.
   f. Select **Add**.
5. To insert a table into the report, move the cursor at the point where you want to insert data.
   a. Select the **Table** tab on the right side pane.
   b. The **Business domain** field is set to **Risk**.
   c. In the **Reporting item** field, select the reporting configuration that you want to insert.
   d. Select **Add**.
   The data is inserted in to the report document. The inserted text takes the formatting of the document. You can modify the formatting as required.
6. To insert a chart, move the cursor at the point where you want to insert the chart.
   a. Select the **Chart** tab on the right side pane.
   b. The **Business domain** field is set to **Risk**.
   c. In the **Reporting item** field, select the reporting configuration that you want to insert.
   d. Select **Add**.
   The chart is inserted in to the report document. The inserted chart can be modified according to your preferences. For example, you can change the colors, the type of chart and so on.
7. To view the details of any record that is inserted in the document, select the content control, and then select **Open link**.
   It takes you to the ServiceNow instance, where you can access the data.
8. To view the list of all ServiceNow links that you've inserted in the report and obtain the latest data on the document, select **Manage Links**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select the check boxes for the links that you want to refresh.

b. Select the refresh icon.
The data is refreshed while displaying the time of refresh and retaining the formatting of the document.

9. To identify and highlight which content control is selected on the report, select the three vertical dots or the more actions icon.
The content control is highlighted in the right pane.

## Using Risk Management

You can use the features and capabilities of the Risk Management application perform various activities such as creating issues, reporting risk events, performing risk assessments and so on.

### Mobile experience for GRC Risk Management

As a risk manager, use your Android or iOS mobile device to manage your work.

### Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

### Overview

As a user with the Now Platform® risk manager (sn_risk.manager) role, manage your tasks, assignments, requests, approvals, and other follow-up actions all from your mobile device. Receive timely notifications for current alerts, as well as risk and compliance status for all your critical assets, vendors, and impacted essential business services.

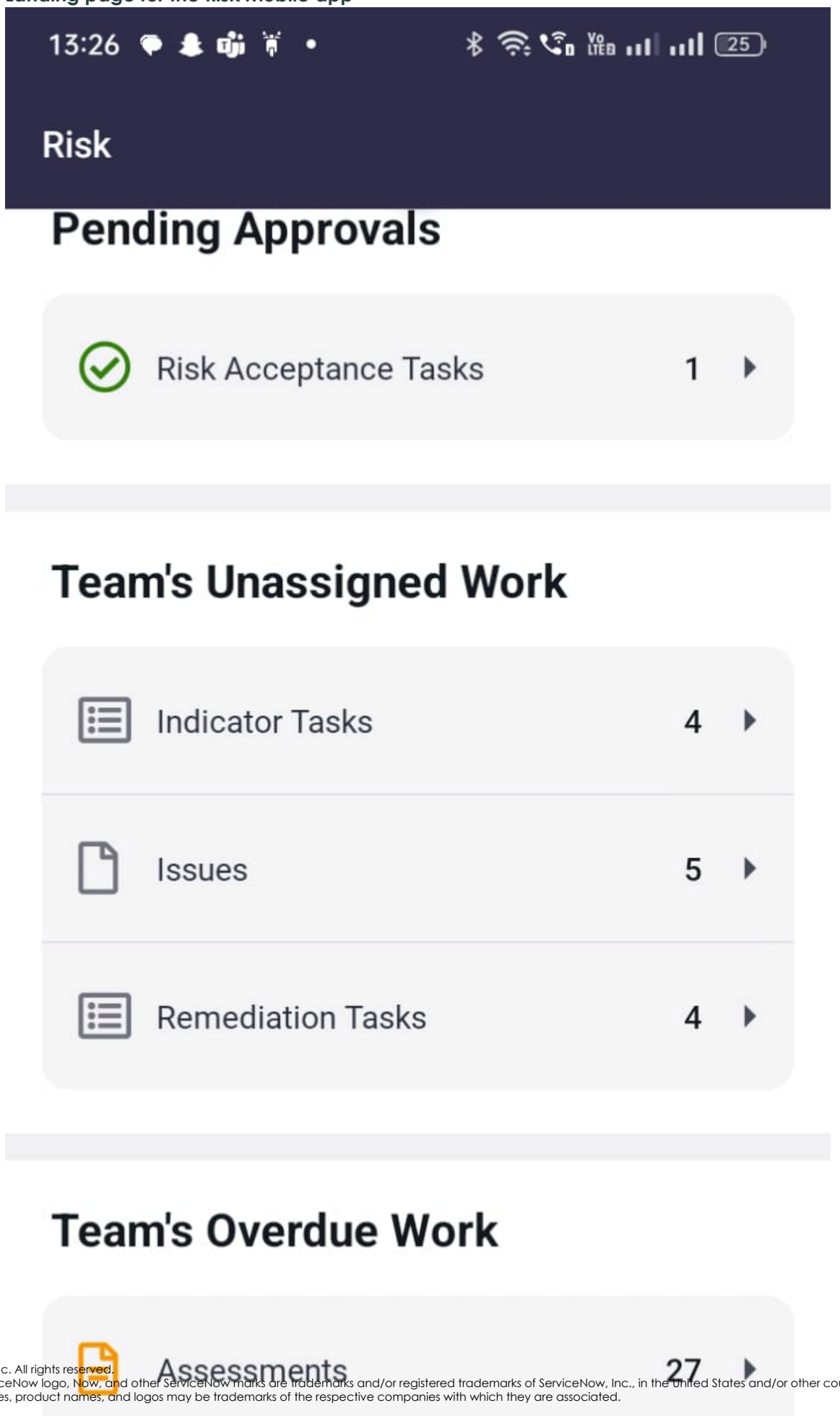
With the GRC Mobile application, you can perform the following Risk Management activities without being tied to the desktop:

- Approve or reject pending tasks that are assigned to you with the Risk Acceptance Tasks applet.
- Assign unassigned tasks to your team with the Indicator Tasks, Issues, and Remediation Tasks applets.
- Manage and reassign your team's overdue tasks with the Assessments and overdue Issues applets.

The following figure illustrates how you log in to your Now Platform instance from your mobile device and the landing screen that is displayed after you log in.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Landing page for the Risk Mobile app**



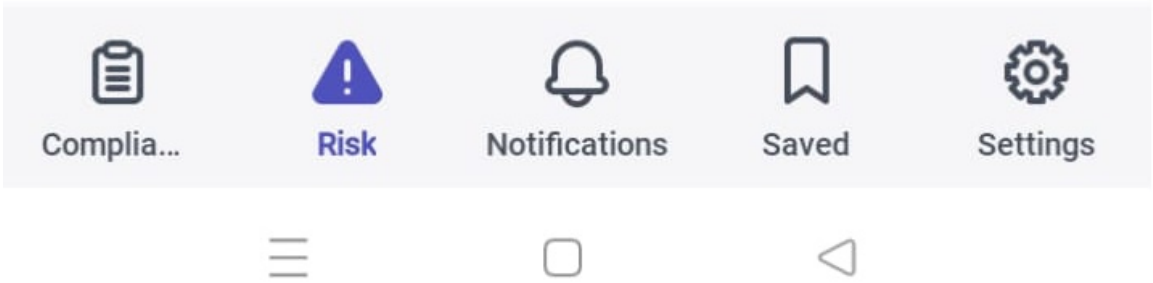

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For step-by-step instructions about how to set up your Now Platform instance and install the GRC Mobile application, see Set up checklist for the GRC Mobile application. For instructions about how to log in, see Log in to the GRC Mobile application.

Applications

Applications are the ServiceNow® software components such as Policy and Compliance Management, Risk Management, and Audit Management that provide specific features and functionalities within your Now Platform instance. After you install these core applications and the GRC Mobile app on your Now Platform instance, these applications are displayed as icons on the bottom of your Android or iOS mobile device after you log in.

**Icons on the bottom of the device screen**




Folders

Each ServiceNow® mobile application contains folders that separate the applets by categories. In the preceding image, Pending Approvals, Team's Unassigned Work, and Team's Overdue Work are the folders of the Risk Mobile app.

Applets

Applets are the different options within the application. In the preceding image, the icons under the Pending Approvals, Team's Unassigned Work, and Team's Overdue Work sections are the available applets for the Risk Mobile app.

### Log in to the GRC Mobile application

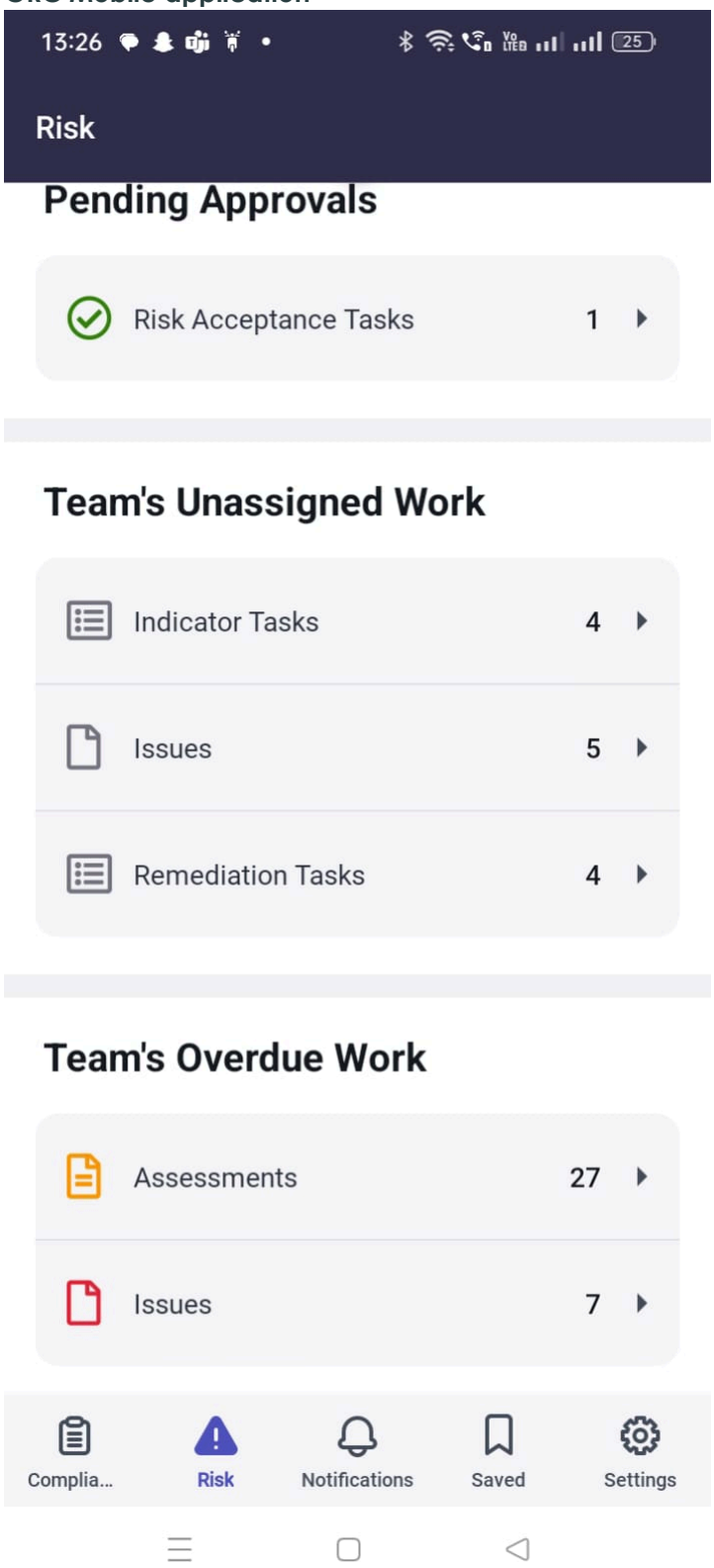
Open the GRC Mobile application and add a Now Platform® instance with Risk Management to your mobile device.

**Before you begin**

Verify that you have completed the setup steps described in Set up checklist for the GRC Mobile application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**GRC Mobile application**




Role required: GRC Risk manager (sn_risk.manager)

**About this task**

Time to complete this task: 5-7 minutes.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. On your mobile device, tap the **ServiceNow Agent** app.

   If you are not already logged in to a Now Platform instance, the Instances screen is displayed.

2. If the Now Platform instance with the Risk Management core application is not already added to your mobile device, follow these steps to add it.

   a. On the Instances screen that is displayed, tap the plus icon (  ).
   A screen is displayed that prompts you to enter and save an address of a Now Platform instance.

   b. Fill in the fields.

| Field | Description |
|---|---|
| Enter the instance address or scan a QR code. | Choose one to continue:<br>▪ Before the `.service-now.com`, enter the name of your Now Platform instance, for example, `grcmobile`.<br>▪ Enter an address in this field. This address is the URL of your Now Platform instance that you want to view on your mobile device, for example, `https://grcprkny.service-now.com`.<br>▪ Scan a QR code.<br>For more information about the mobile app, see Log in to an instance with a mobile app |
| (Optional) Enter nickname | Enter a nickname for this instance. If you have multiple instances added to the device, nicknames can help you quickly locate a Now Platform instance. |

   c. Tap **Save and Login**.

3. On the ServiceNow login screen that is displayed, enter the User name and Password for the Now Platform instance that you want to add and tap **Login**.
   The Risk landing screen is displayed. You have successfully logged in to the GRC Mobile application.

4. After you log in, verify notifications are enabled in the GRC Mobile application.

   a. On the landing screen on the bottom, tap **More**.

   b. On the More screen, tap **Notification**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. On the Notifications screen, tap **Enable Notifications** if not enabled.
Notifications from the Now Platform are displayed on the Notifications screen in the GRC Mobile application.

5. After you login to an instance on your mobile device, it is the default Now Platform instance on the device.
If you want to view another Now Platform instance on the device, you must log out of the default instance. To log out:

a. Tap the **More**.
The More screen is displayed.

b. Tap **Settings**.

c. On the screen that is displayed, tap **Logout**.
The Instances screen is displayed with any Now Platform instances you have added to the mobile device.

d. Optional: Tap another instance to log in to it, or, alternatively, follow the preceding steps to add another instance.

**Trouble?**

If the instances screen for the GRC Mobile application is not displayed after you tap the **ServiceNow Agent** app on your device, verify that the **ServiceNow Agent** is permitted as a trusted app on your device. To permit access as a trusted app, navigate to the settings or general device management area on your mobile device and tap the option (**Trust app**, etc.) to permit access.

If an error message is displayed after you enter your credentials in the log in screen, verify that your User name and password for the Now Platform instance is correct.

If you have problems viewing the landing screen, verify your network connection.

If you cannot view the Instances screen after you tap the **ServiceNow Agent** app, try uninstalling it from your device. Verify you have the most current version of the app from the Apple iOS App Store or the Google Play Store and try reinstalling it.

## What to do next

Select one of the following topics for more information about each applet.

### Process pending Risk acceptance tasks with the GRC Mobile application

Process pending approval requests for Risk Management acceptance tasks that are submitted to you.

## Before you begin

Role required: GRC risk manager (sn_risk.manager)

## About this task

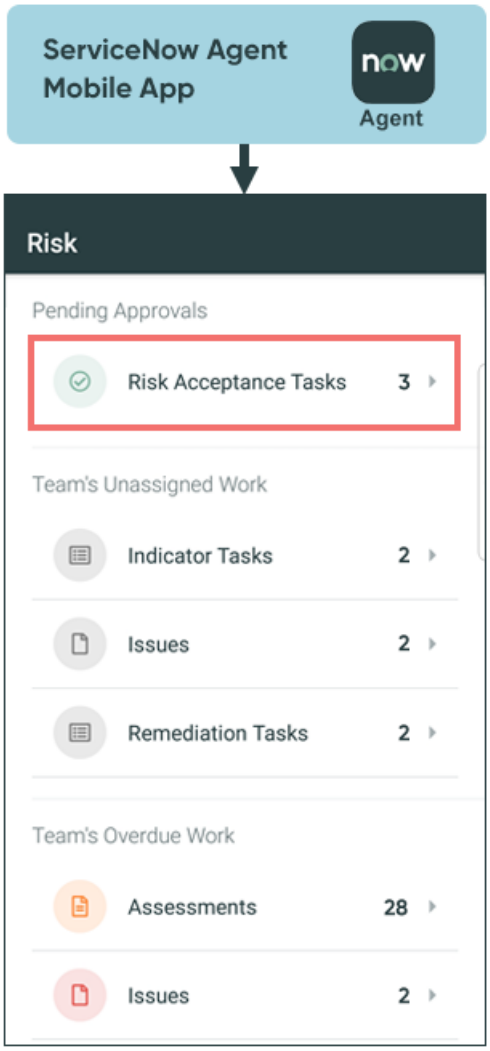
Approve or reject a pending request from the list of records. Alternatively, view the details of the record or add a work note prior to processing the request. Time to complete this task: 5-10 minutes.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

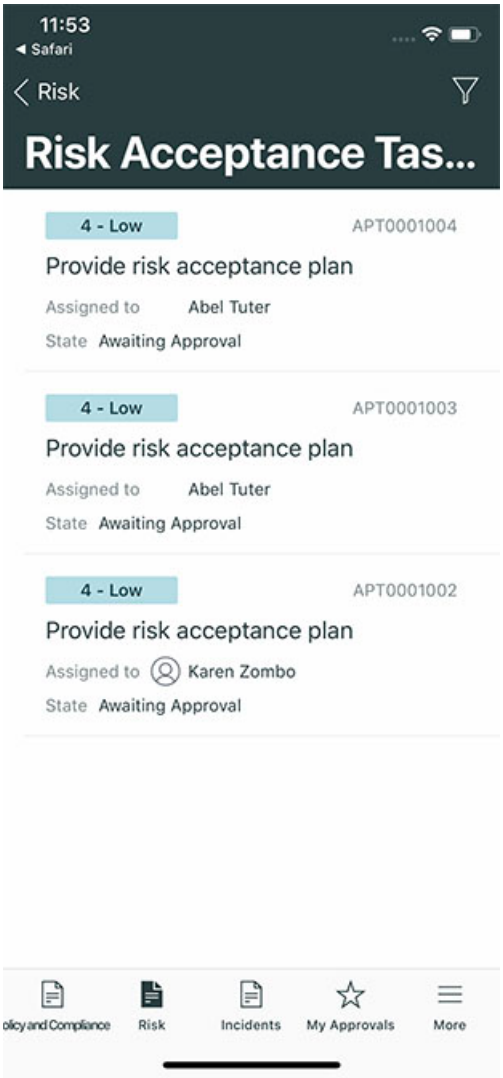
1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Risk landing screen displayed, tap **Risk Acceptance Tasks**.

   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.




The Risk Acceptance Tasks screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

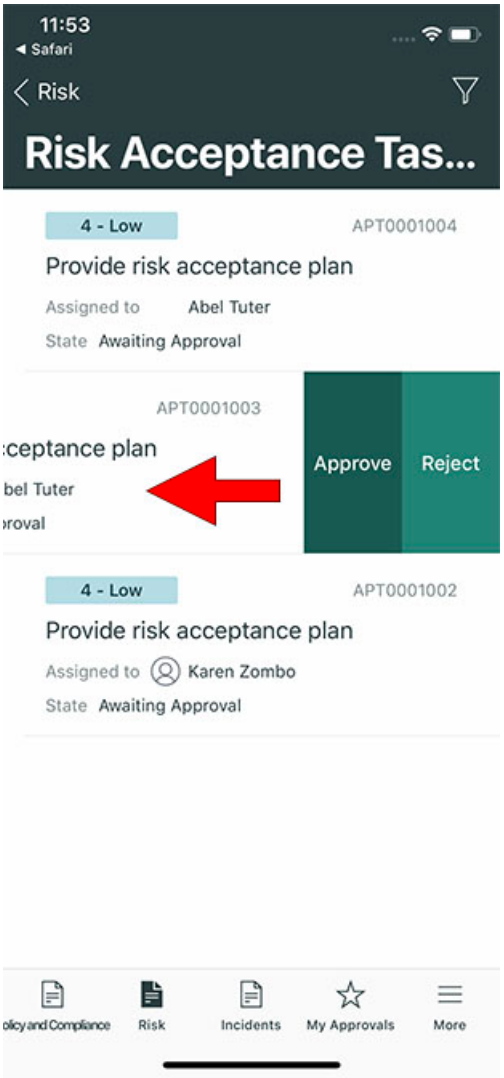



3. Optional: If you want to reduce the number of records that are displayed on the screen, see Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

4. To approve or reject a request directly from the list, with the Risk Acceptance Tasks screen displayed, swipe left on a record to open the menu.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



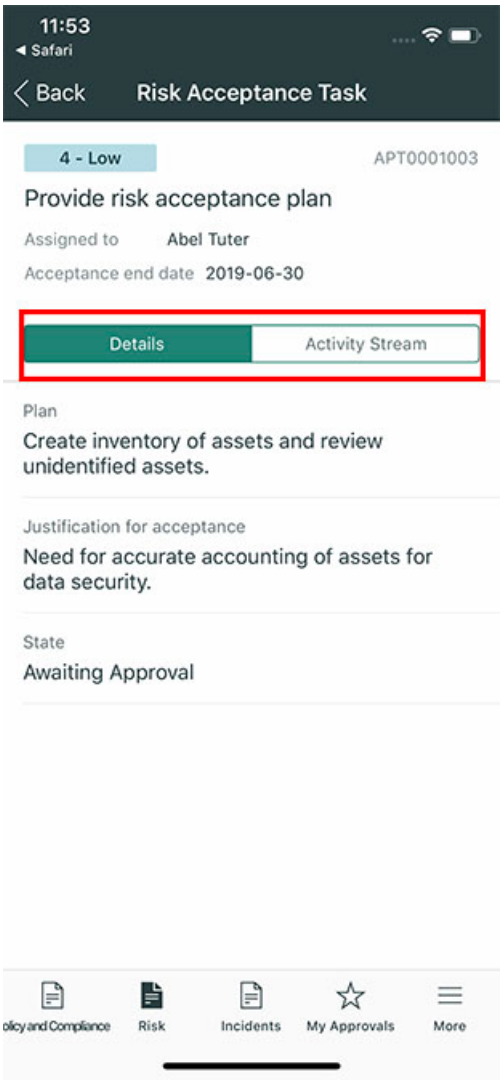

5. On the menu that is displayed, choose one to continue.

| Option | Description |
|---|---|
| Approve | In the Comments field, enter comments. Comments are optional for approvals. Tap the Send icon ( ) or **Submit** to save and submit your changes. |
| Reject | In the Comments field, enter comments. Comments are required for rejections. Tap the Send icon ( ) or **Submit** to save and submit your changes. |

6. Alternatively, with the Risk Acceptance Tasks screen displayed, follow these steps to view more details or add a work note to a record on the list.
7. With the Risk Acceptance Task screen displayed, tap the record to open it.
8. To view more details, on the record that is displayed, tap **Approval for** to view the Risk Acceptance Task.
9. Tap the task record that is displayed to open it.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

On the record that is displayed, choose one from the following table to continue.




| Option | Description |
| --- | --- |
| Details tab | With the Details tab selected, to approve or reject the request, at the top left of the screen, tap the back arrow icon  two times to navigate back to the Risk Acceptance Task record. With the Risk Acceptance Task screen displayed, tap the menu icon (  ) to approve or reject the request. Follow the steps described in the preceding table. |
| Activity Stream tab | With the Activity Stream tab selected, follow these steps. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | **a.** View the work notes and additional comments. To add a work note or attach a file, tap the plus icon (  ). |
| | **b.** Navigate back to the Risk Acceptance Task record as described in the preceding option and tap the menu icon (  ) to approve or reject the request. |
| Tap a screen icon at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br>◦ Tap the Risk icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br>◦ Tap **More**:<br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **More** followed by **Settings**. Tap **Log out** to log out of the current instance. |

### Assign Risk Management indicator tasks with the GRC Mobile application

Assign unassigned indicator tasks to a member of your assignment group. An indicator task is related to a Risk record that is assigned to your compliance group.

#### Before you begin

Role required: GRC Risk manager (sn_risk.manager)

#### About this task

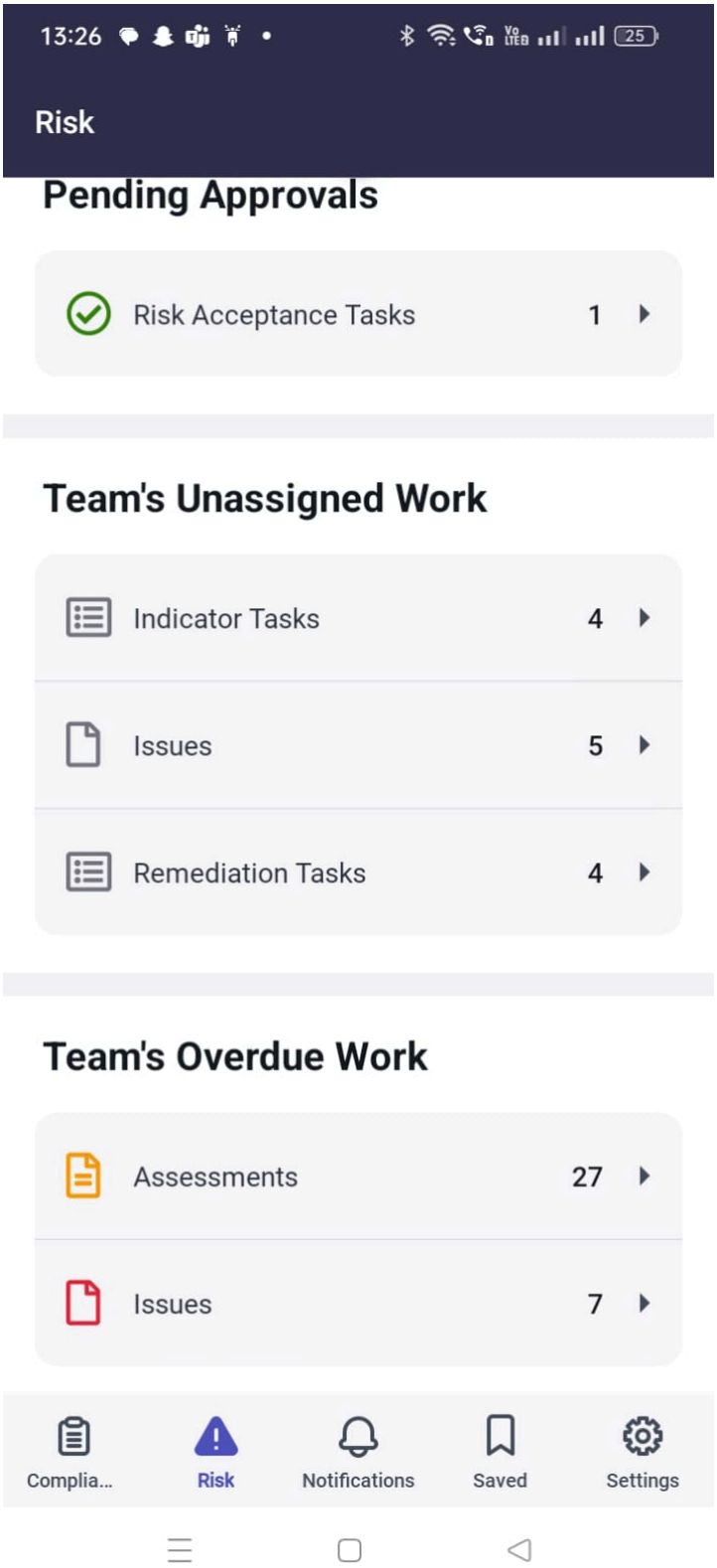
Assign an Indicator Task from the list of records. Alternatively, view the details of the record or add a work note prior to assignment. Time to complete this task: 5-10 minutes.

#### Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Risk landing screen displayed, under the `Team's Unassigned Work` section, tap **Indicator Tasks**.

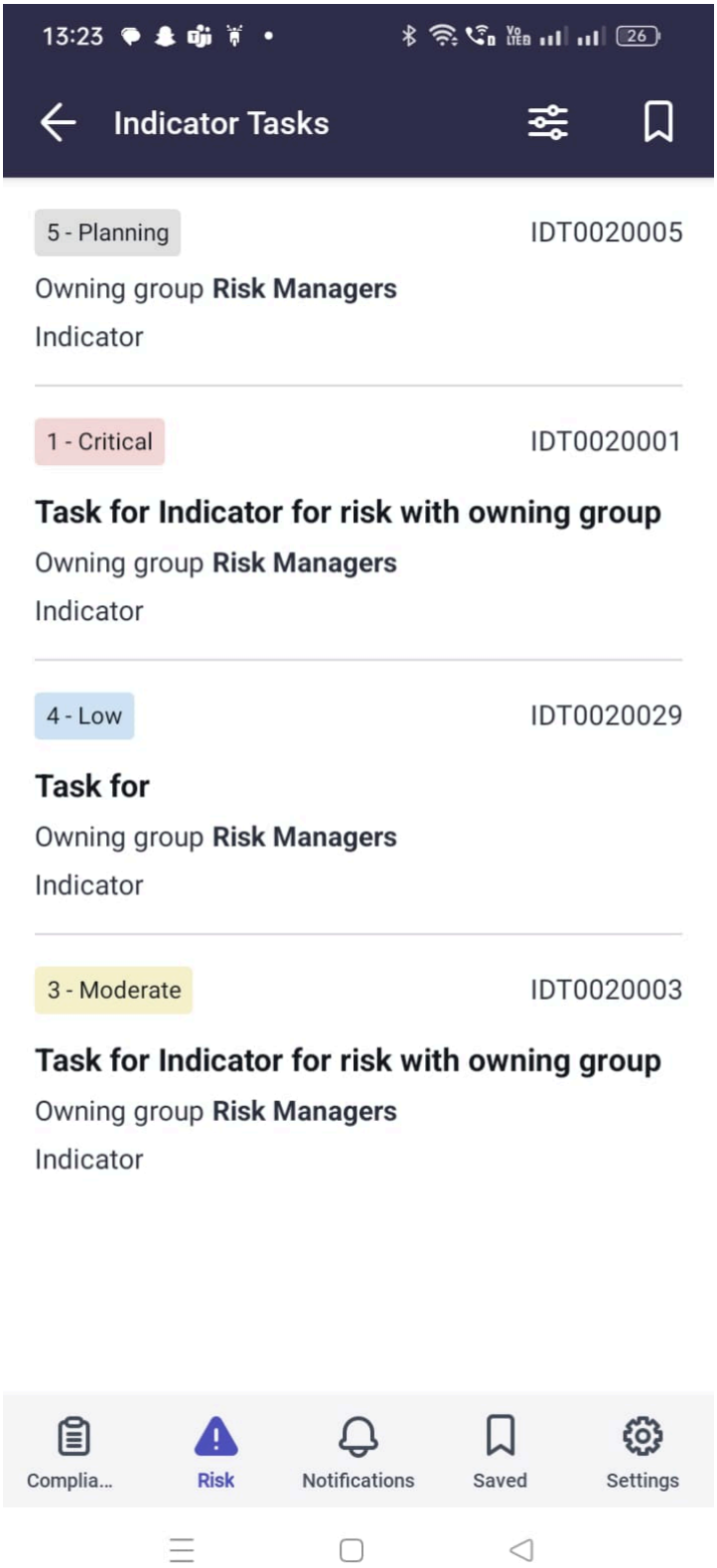
   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The Indicator Tasks screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

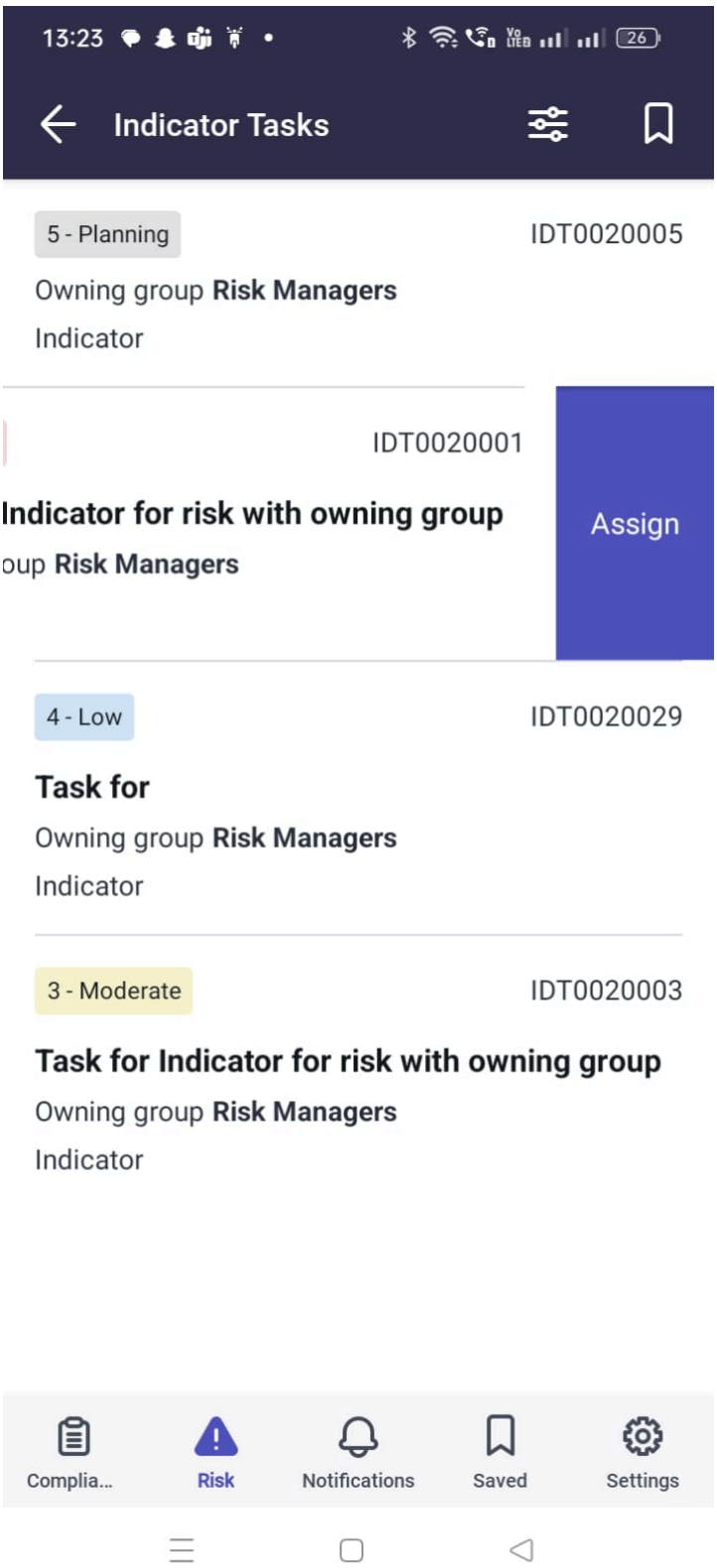



3. Optional: If you want to reduce the number of records that are displayed on the screen, see Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To assign a task directly from the list of records displayed on the Indicator Tasks screen, swipe left on a record to open the menu.



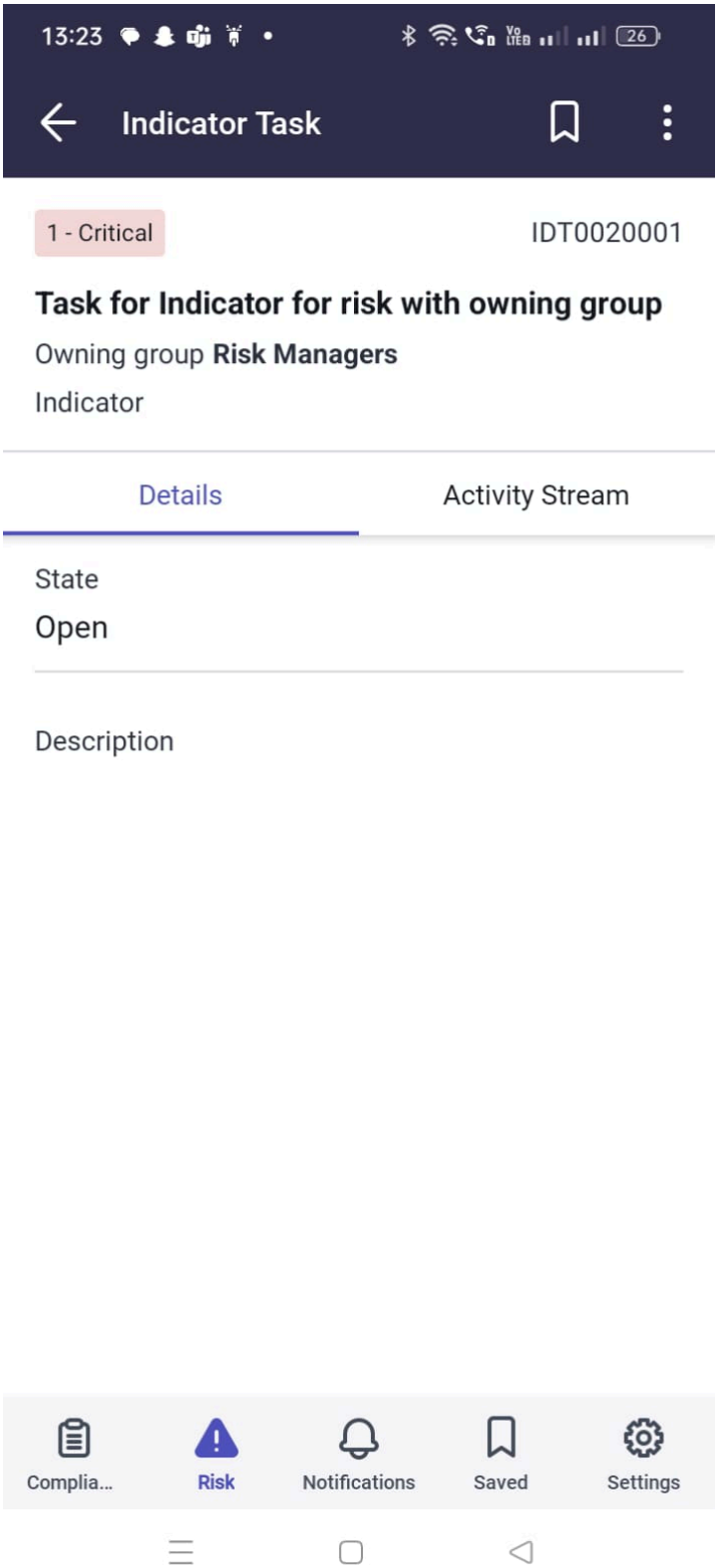

5. Tap **Assign**.
6. Tap **Assigned to**, and, on the screen that is displayed, tap a user. Alternatively, enter text in the Search field.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The name of the user is displayed on the Assign Indicator Task screen. You can assign indicator tasks to any user.

7. Tap the Send icon ( ) or **Submit** to save and submit your changes.
   After you assign the task to a user, the record is no longer displayed on the Indicator Tasks list.
8. Alternatively, to review more details or add work notes, with the Assign Indicator Task screen displayed, tap a record on the list to open it.
9. With the fields on the record displayed, choose one in the following table to continue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




| Option | Description |
| --- | --- |
| Details tab | With the Details tab selected, to assign the record, at the top right of the screen, tap the menu icon ( ). Follow the steps described in the preceding table. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| Activity Stream tab | With the Activity Stream tab selected, choose one to continue.<br>◦ View work notes and additional comments. Tap the plus icon (  ) to add a work note or attach a file.<br>◦ At the top right of the screen, tap the menu icon (  ). Tap Assign. On the screen that is displayed, tap a user. Alternatively, enter text in the Search field. Tap the send icon (  ) or **Submit** to save and submit your changes. |
| Tap a screen icon at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br>◦ Tap the Risk icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br>◦ Tap **More**:<br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **More** followed by **Settings**. Tap **Log out** to log out of the current instance. |

### Assign Risk Management issues with the GRC Mobile application

Assign unassigned issues to a member of your assignment group. Navigate through the record to view more details about the Risk Statement, the Risk record, and Remediation Tasks associated with an issue.

## Before you begin

Role required: GRC risk manager (sn_risk.manager)

## About this task

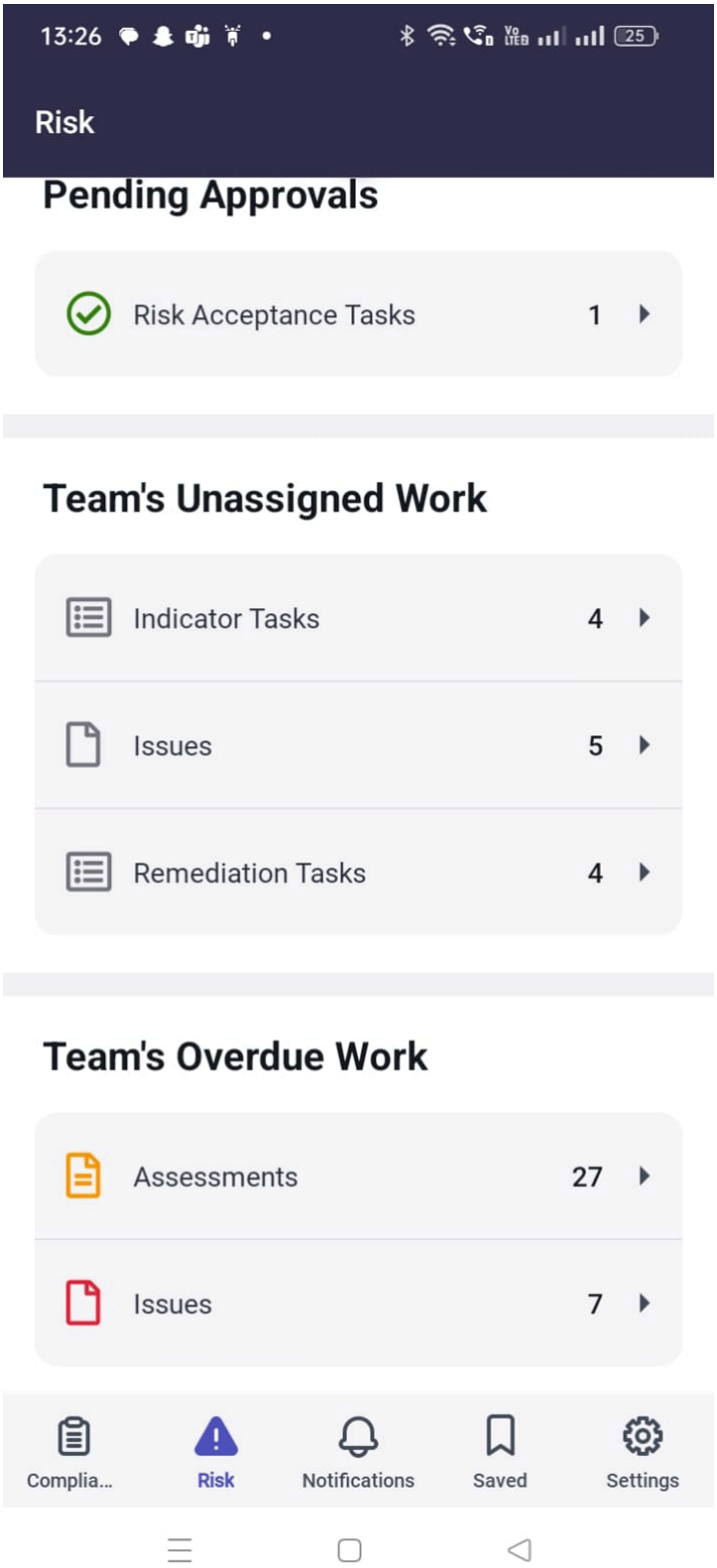
Edit or assign an issue from the list of records. Alternatively, add or work note or view the details and related lists of the record prior to assignment. Time to complete this task: 5-10 minutes.

## Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Risk landing screen displayed, under the `Team's Unassigned Work` section, tap **Issues**.

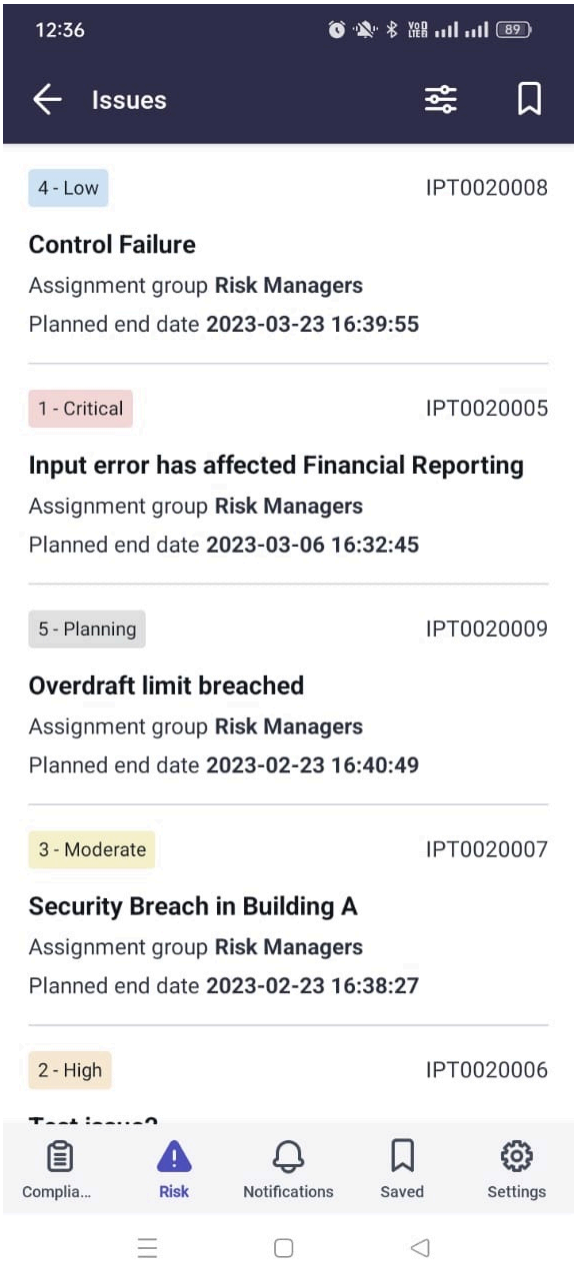
   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The Issues screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

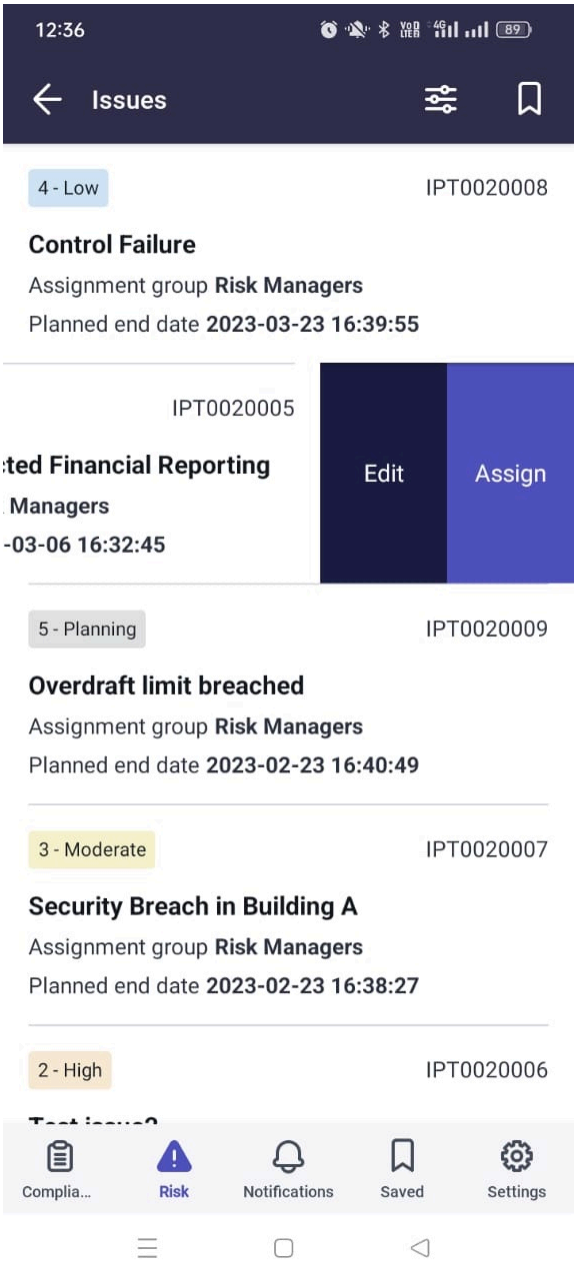



3. Optional: If you want to reduce the number of records that are displayed on the screen, see Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

4. To edit or assign an issue directly from the list of records displayed on the Issues screen, swipe left on a record to open the menu.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

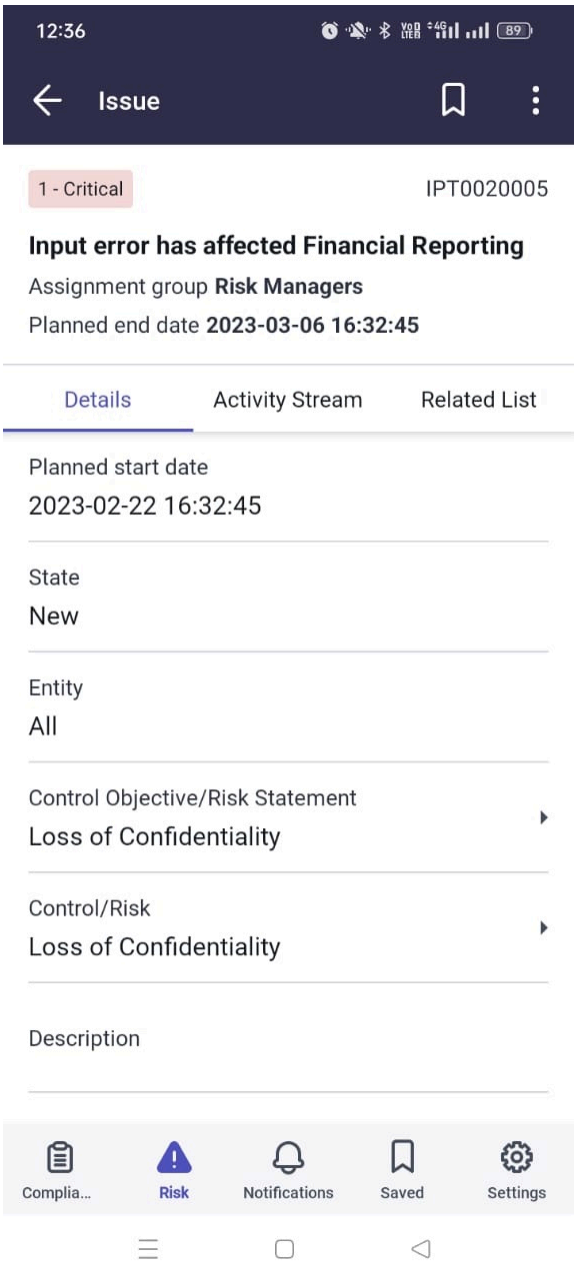



**5.** In the menu that is displayed, choose one from the following table to continue.

| Option | Description |
|---|---|
| Edit | In the Extend by days field on the Edit Issue screen that is displayed, enter a value. This value is added to the Duration field in your Now Platform instance. Tap the Send icon ( ) or **Submit** to save and submit your changes. |
| Assign | On the Issue Assignment screen that is displayed, tap the **Assignment Group** and **Assigned to** fields to assign the issue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. Alternatively, with the Issues screen displayed, tap a record on the list to open it and view more details.
7. With the fields on the issue record displayed, choose one in the following table to continue.




| Option | Description |
| --- | --- |
| Details tab | With the Details tab selected, choose one to continue.<br>◦ View the fields for details about the issue, especially the planned start and end dates.<br>Tap the **Control Objective/Risk Statement** field to expand it. A list of Risk Statement records is displayed. Tap an item to display the Risk Statement record. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | Tap the **Control/Risk** field to expand it. A list of Risk records is displayed. Tap an item on the list to open the record. With the record displayed, select the **Details** or **Activity Stream** tabs for more information.<br>◦ At the top right of the screen with the Issue screen displayed, tap the menu icon (  ) to edit and assign the issue. Follow the steps described in the preceding table. |
| Activity Stream tab | With the Activity Stream tab selected, choose one to continue.<br>◦ View work notes and additional comments. Tap the plus icon (  ) to add a work note or attach a file.<br>◦ At the top right of the screen, tap the menu icon (  ) to assign or edit the issue. Follow the steps described in the preceding table. |
| Related List tab | With the Related List tab selected, follow these steps.<br>**a.** Tap **Remediation Tasks** to expand the field. On the Remediation Task screen, view the items on the related list that are associated with the Issue record.<br>**b.** On the list that is displayed, tap an item to open the record and view more details about the task.<br>**c.** After your review, with navigate back to the issue record and tap the menu (  ) to assign or edit the issue. Follow the steps described in the preceding table. |
| Tap a screen icon at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br>◦ Tap the Risk icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br>◦ Tap **More**:<br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **More** followed by **Settings**. Tap **Log out** to log out of the current instance. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Assign Risk Management remediation tasks with the GRC Mobile application

Assign an unassigned remediation task to a user of your group. Edit the fields including the **Extend by days** field. Navigate through the record to view more details about the Risk Statement, the Risk record, and the Issues associated with a Remediation Task.

#### Before you begin

Role required: GRC Risk manager (sn_risk.manager)

#### About this task

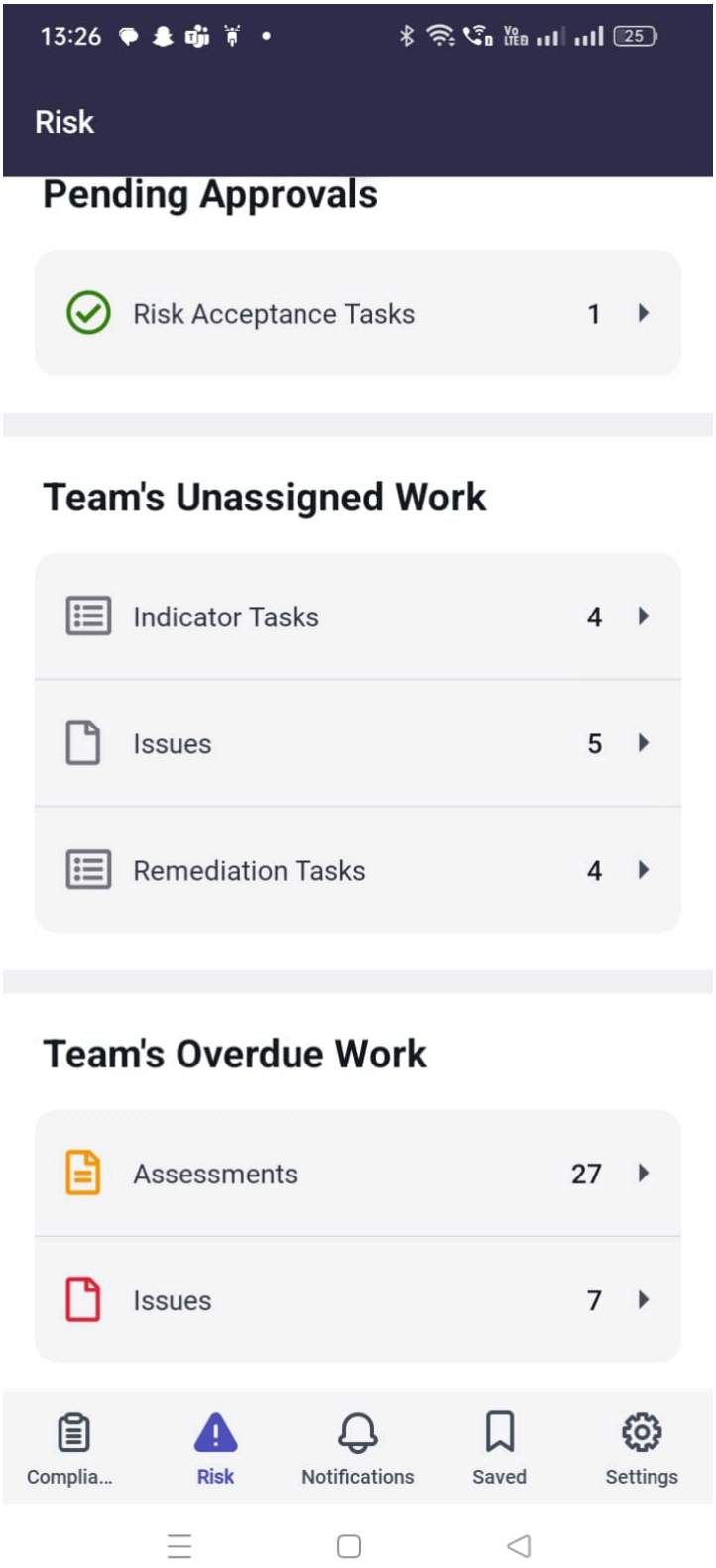
Edit or assign an unassigned remediation task directly from the list of records. Alternatively, view the details of the record prior to assignment or add a work note. Time to complete this task: 5-10 minutes.

#### Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Risk landing screen displayed, under the `Team's Unassigned Work` section, tap **Remediation Tasks**.

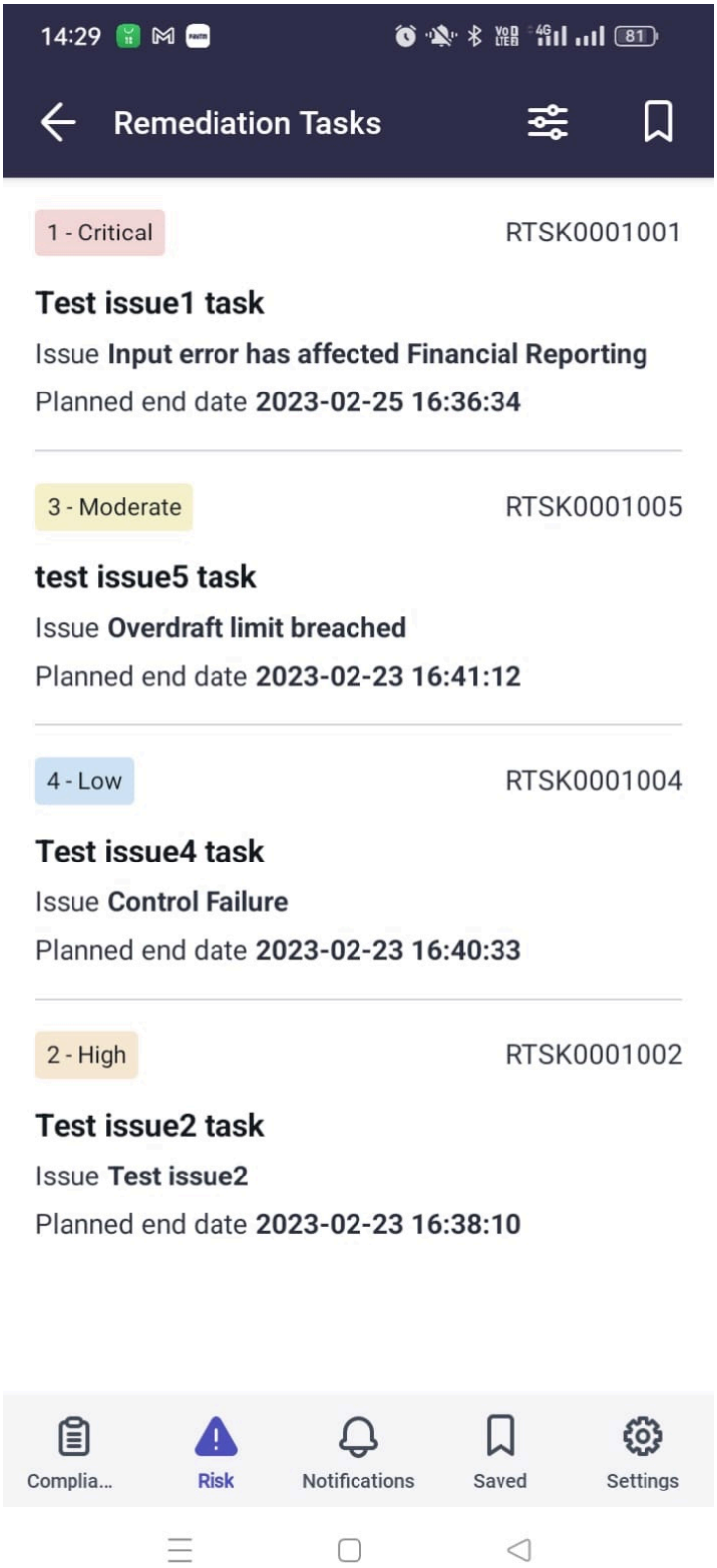
   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The Remediation Tasks screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

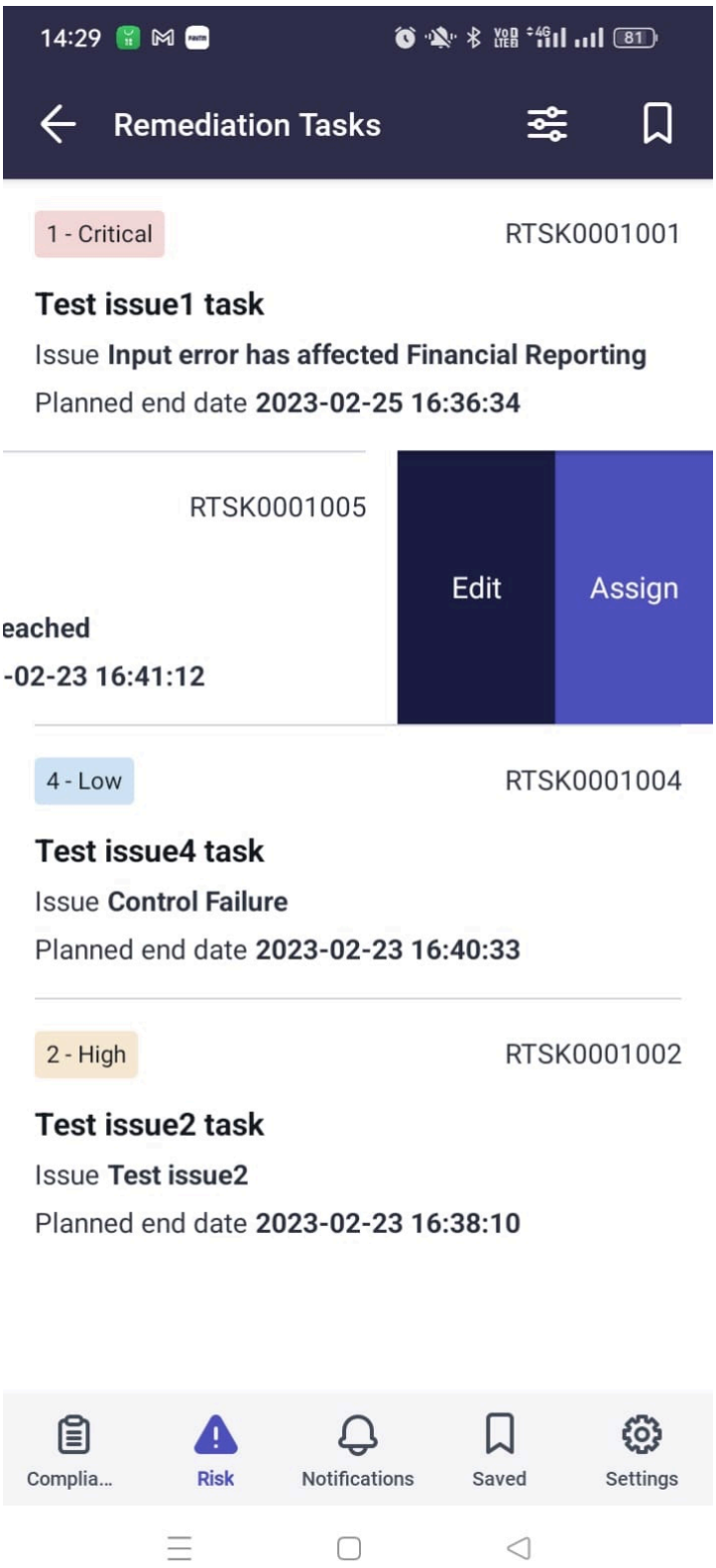



3. Optional: If you want to reduce the number of records that are displayed on the screen, see Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To edit or assign a task directly from the list of records displayed on the Remediation Tasks screen, swipe left on a record to open the menu.



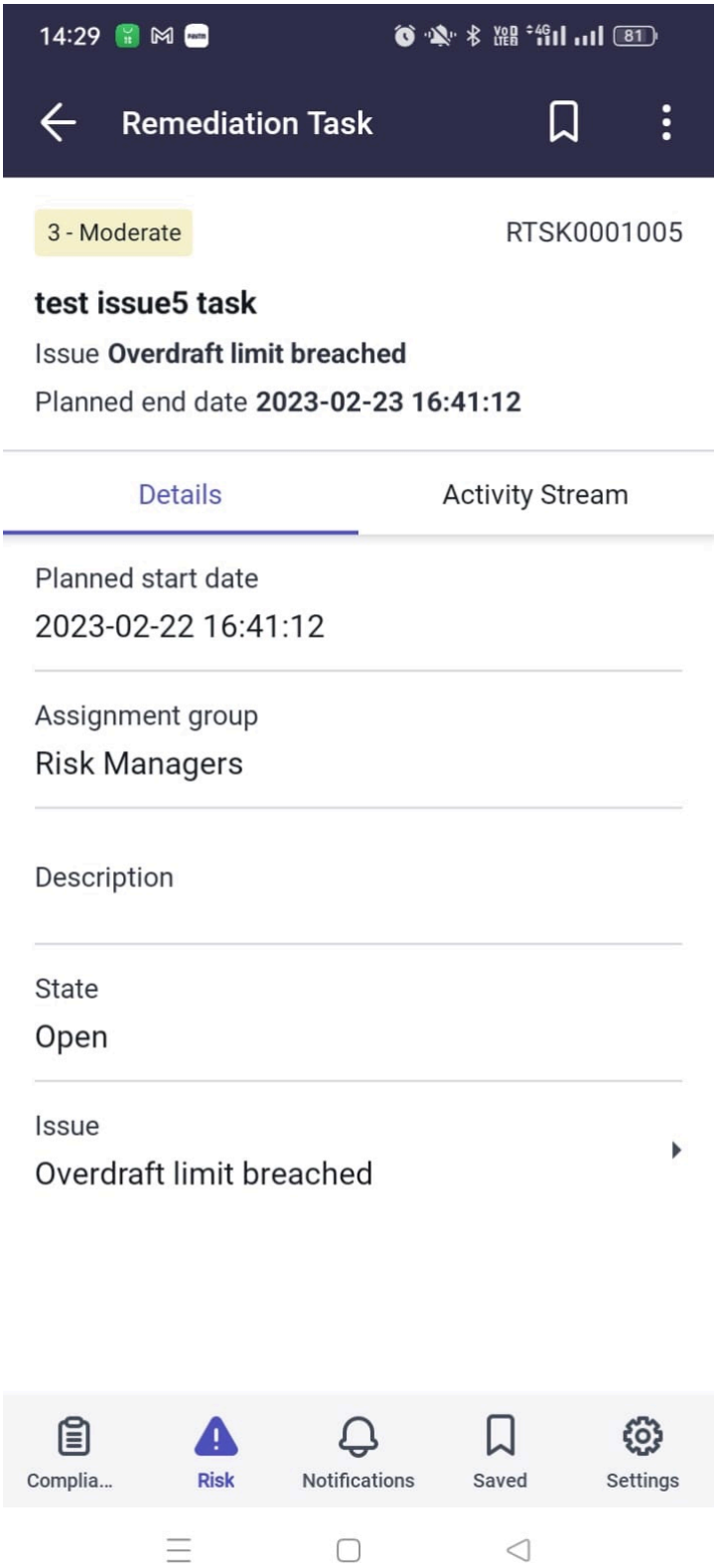

5. In the menu that is displayed, choose one to continue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| Edit | In the Extend by days field on the Edit Remediation Task screen that is displayed, enter a value. This value is added to the Duration field in your Now Platform instance.<br><br>To assign the remediation task, tap the Assigned to field and tap a name. Alternatively, enter a user name in the search field.<br><br>Tap the Send icon (  ) or **Submit** to save and submit your changes. |
| Assign | On the Issue Assignment screen that is displayed, tap the **Assignment Group** and **Assigned to** fields to assign the issue. |

6. Alternatively, with the Remediation Tasks screen displayed, tap a record on the list to open it and review more details.
7. With the fields on the issue record displayed, choose one in the following table to continue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




| Option | Description |
| --- | --- |
| Details tab | With the Details tab selected, choose one to continue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | ◦ View the fields for details about the issue, especially the planned start and end dates.<br><br>Tap the **Issue** field to expand it. On the Issue screen, a list of records is displayed. Tap an item to display more details about the Risk Statement and Risk record.<br><br>◦ Navigate back to the Remediation Task record and tap the menu icon (  ) to assign or edit the remediation task. Follow the steps described in the preceding table. |
| Activity Stream tab | With the Activity Stream tab selected, choose one to continue.<br>◦ View work notes and additional comments. Tap the plus icon (  ) to add a work note or attach a file.<br>◦ At the top right of the screen, tap the menu icon (  ) to edit and assign the remediation task. Follow the steps described in the preceding table. |
| Tap a screen icon at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br>◦ Tap the Risk icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br>◦ Tap **More**:<br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **More** followed by **Settings**. Tap **Log out** to log out of the current instance. |

### Reassign overdue Risk Management assessments with the GRC Mobile application

Reassign overdue risk assessments to another member of your assignment group.

#### Before you begin

Role required: GRC Risk manager (sn_risk.manager)

#### About this task

Reassign a risk assessment that is past its due date directly from the list of records. Alternatively, view the details of the record to prior to reassignment. Time to complete this task: 5-10 minutes.

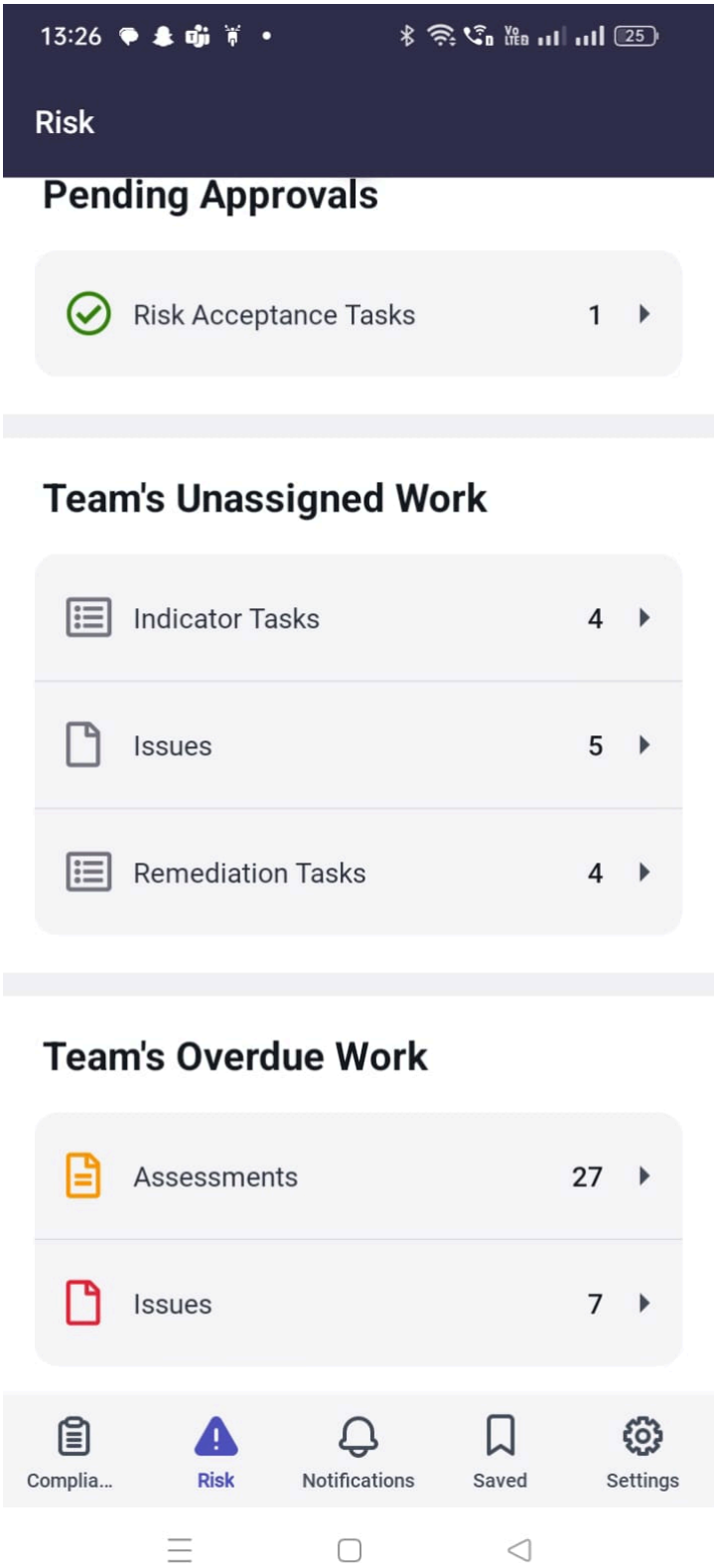
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Risk landing screen displayed, under the `Team's Overdue Work` section, tap **Assessments**.

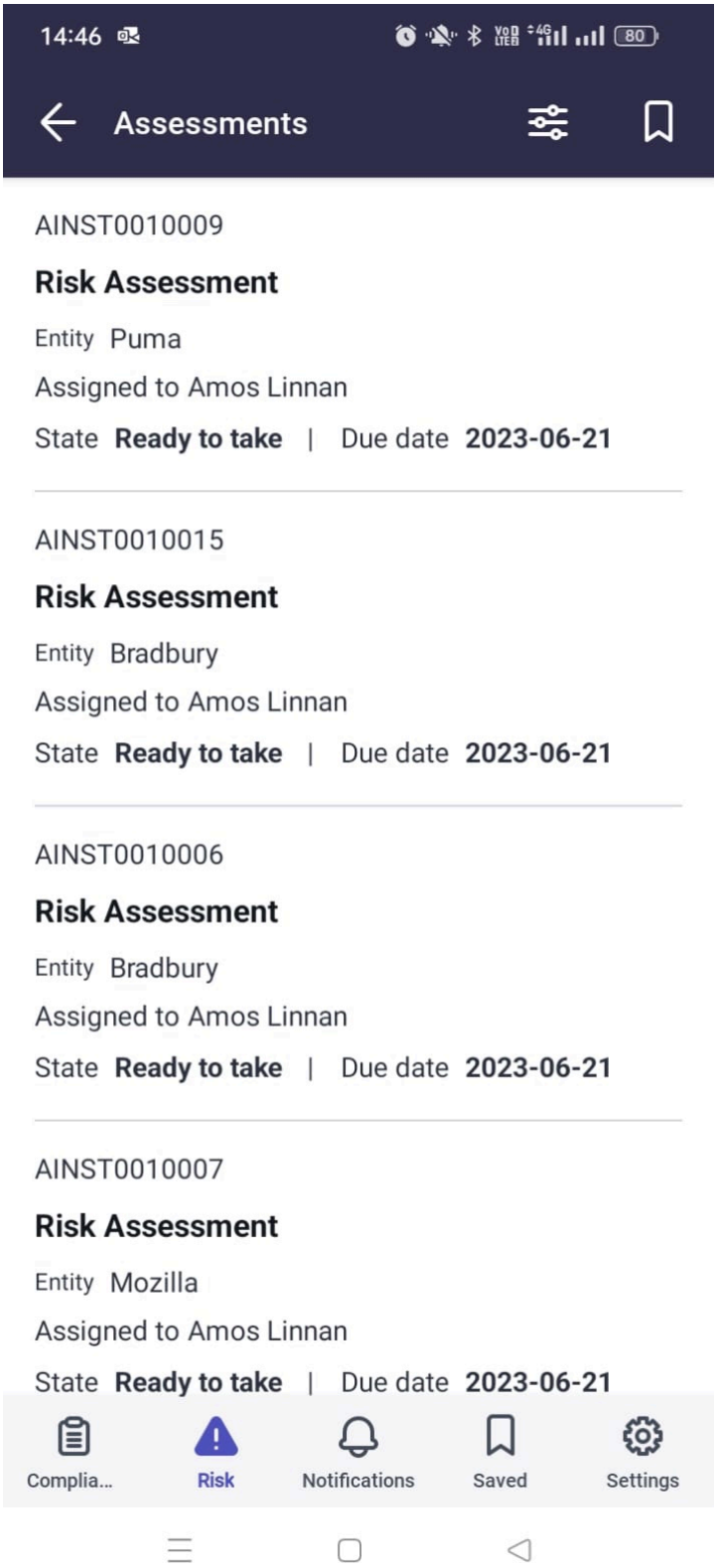
   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The Assessments screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

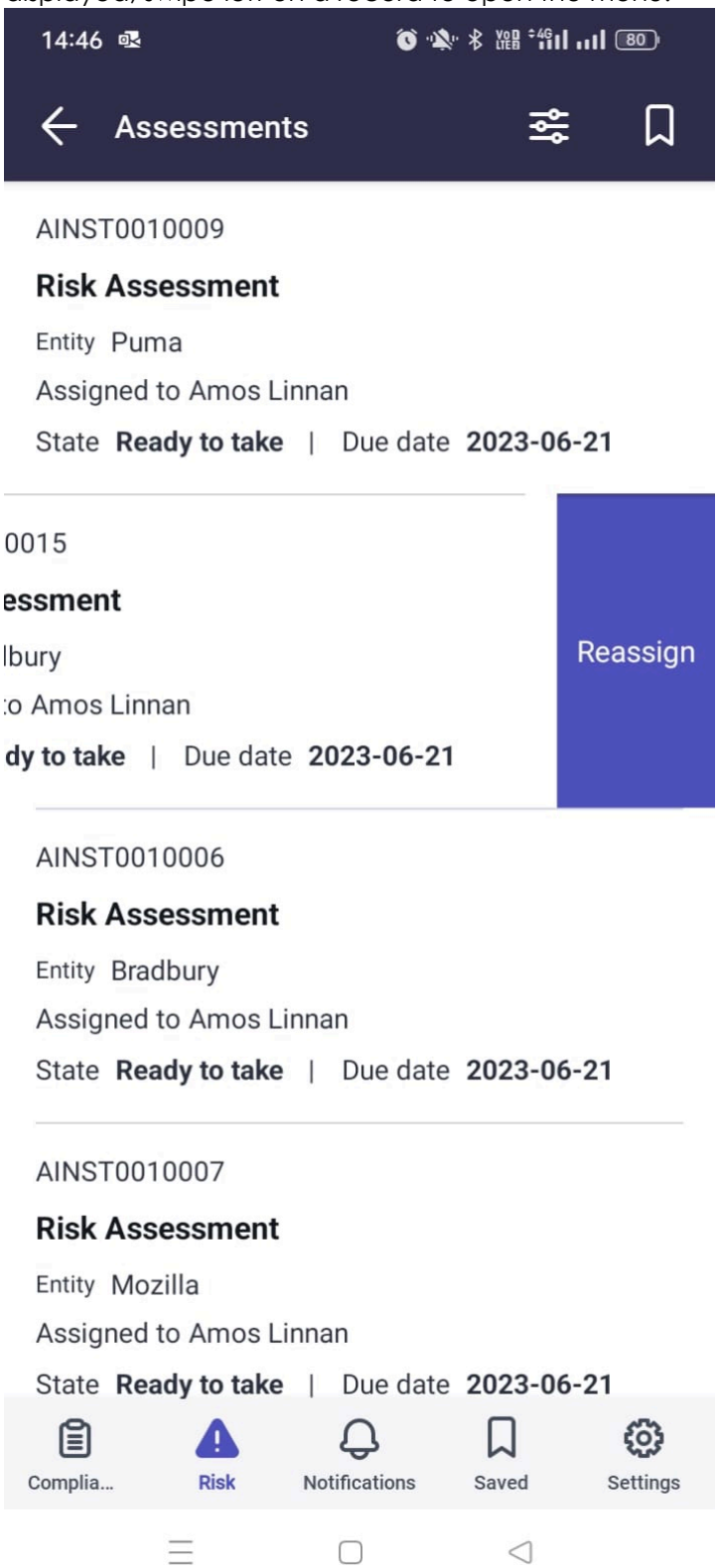



3. Optional: See Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

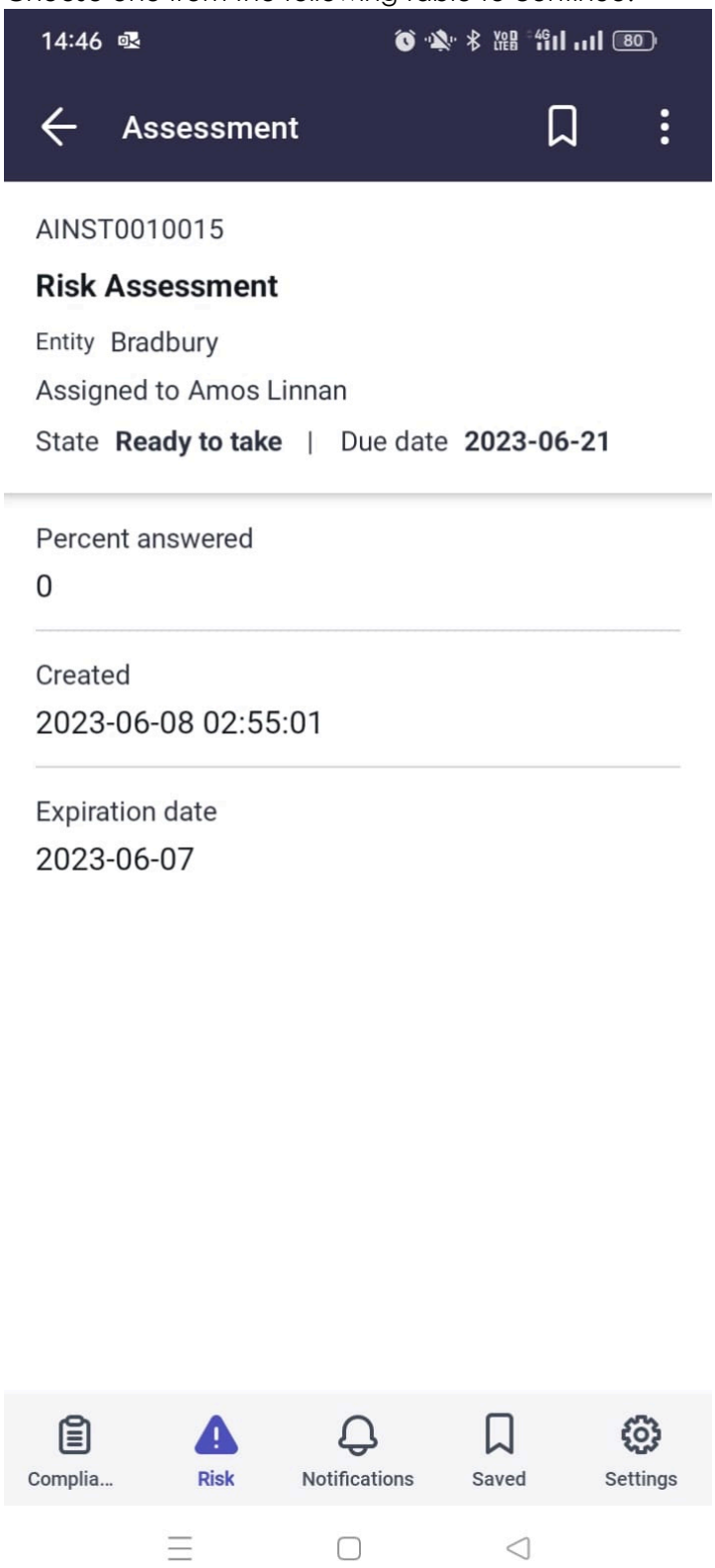
4. To reassign a risk assessment directly from the list of records, with the Assessments screen displayed, swipe left on a record to open the menu.




5. Tap **Reassign**, and, tap the **Assigned to** field.
6. Tap a user name, or, alternatively, enter a name in the search field.
7. Tap the Send icon ( ) or **Submit** to save and submit your changes.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Alternatively, with the Assessments screen displayed, tap a record on the list to open it and view more details.
9. Choose one from the following table to continue.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| Reassign | With the record displayed, review the details and tap the menu icon (  ) to reassign the assessment. |
| Tap a screen icon at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br>◦ Tap the Risk icon to return the landing screen.<br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br>◦ Tap **More**:<br>▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **More** followed by **Settings**. Tap **Log out** to log out of the current instance. |

### Reassign overdue Risk Management issues with the GRC Mobile application

Reassign overdue Risk Management issues that are assigned to your assignment group.

#### Before you begin

Role required: GRC Risk manager (sn_risk.manager)

#### About this task

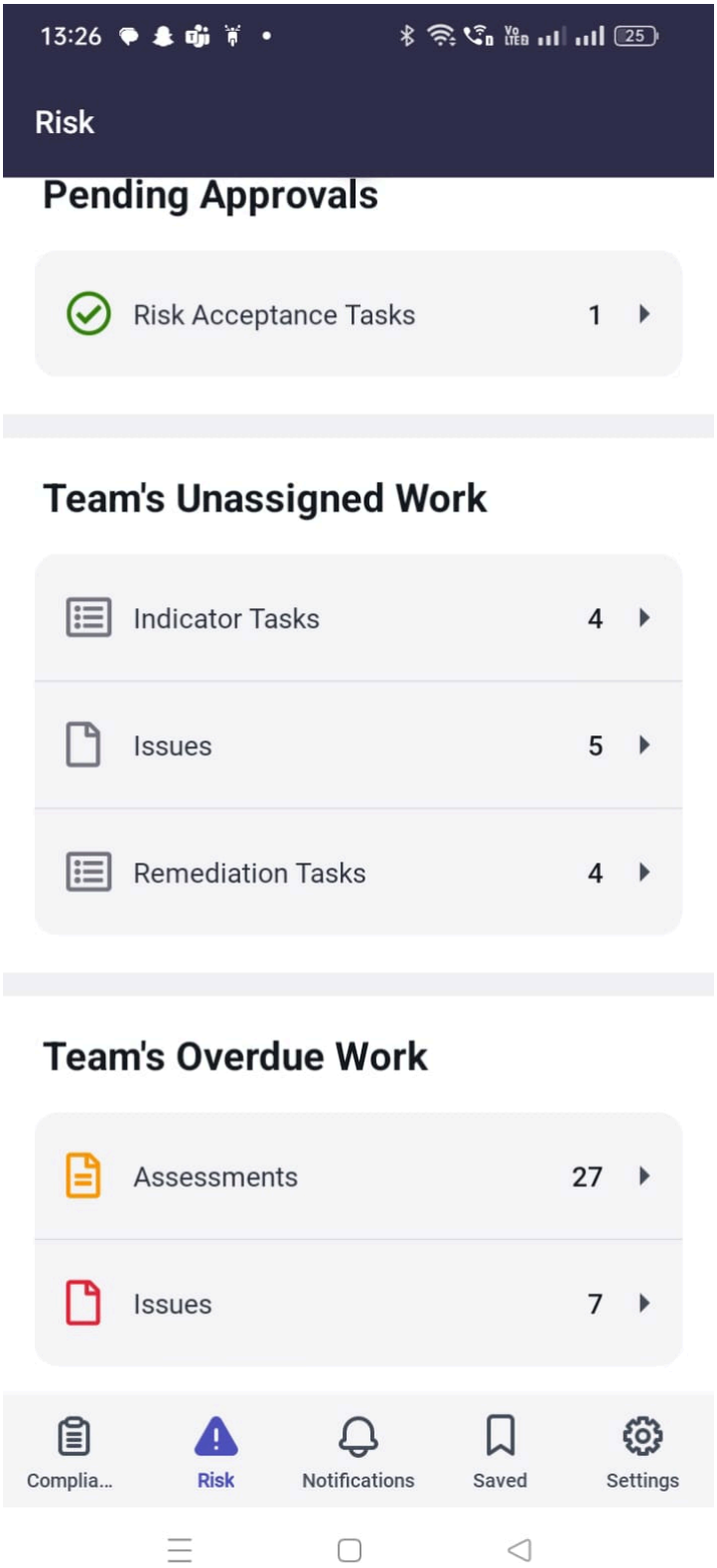
Edit or reassign a task directly from the list of records. Alternatively, add a work note or navigate through the record to view more details about the Risk Statement, the Risk record, and associated Remediation Tasks prior to reassignment. If an issue is not assigned to your assignment group, it is not displayed on this list. Time to complete this task: 5-10 minutes.

#### Procedure

1. If you are not logged in to your Now Platform instance on your mobile device, for more information see Log in to the GRC Mobile application.
2. With the Risk landing screen displayed, under the `Team's Overdue Work` section, tap **Issues**.

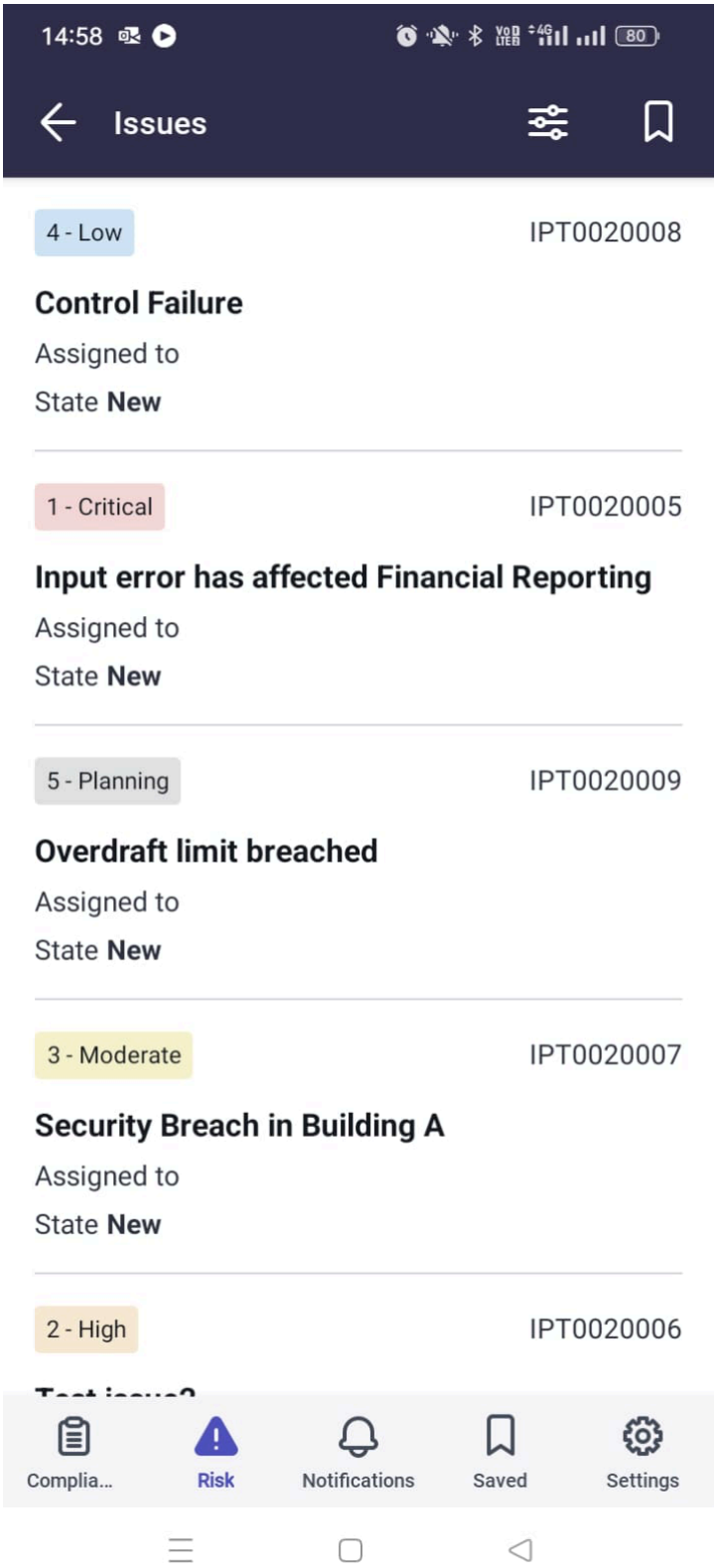
   If you navigate away from the GRC Mobile application after you have logged in, tap the Now Agent app at any time to return to the last screen you had displayed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The Issues screen is displayed with a list of records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

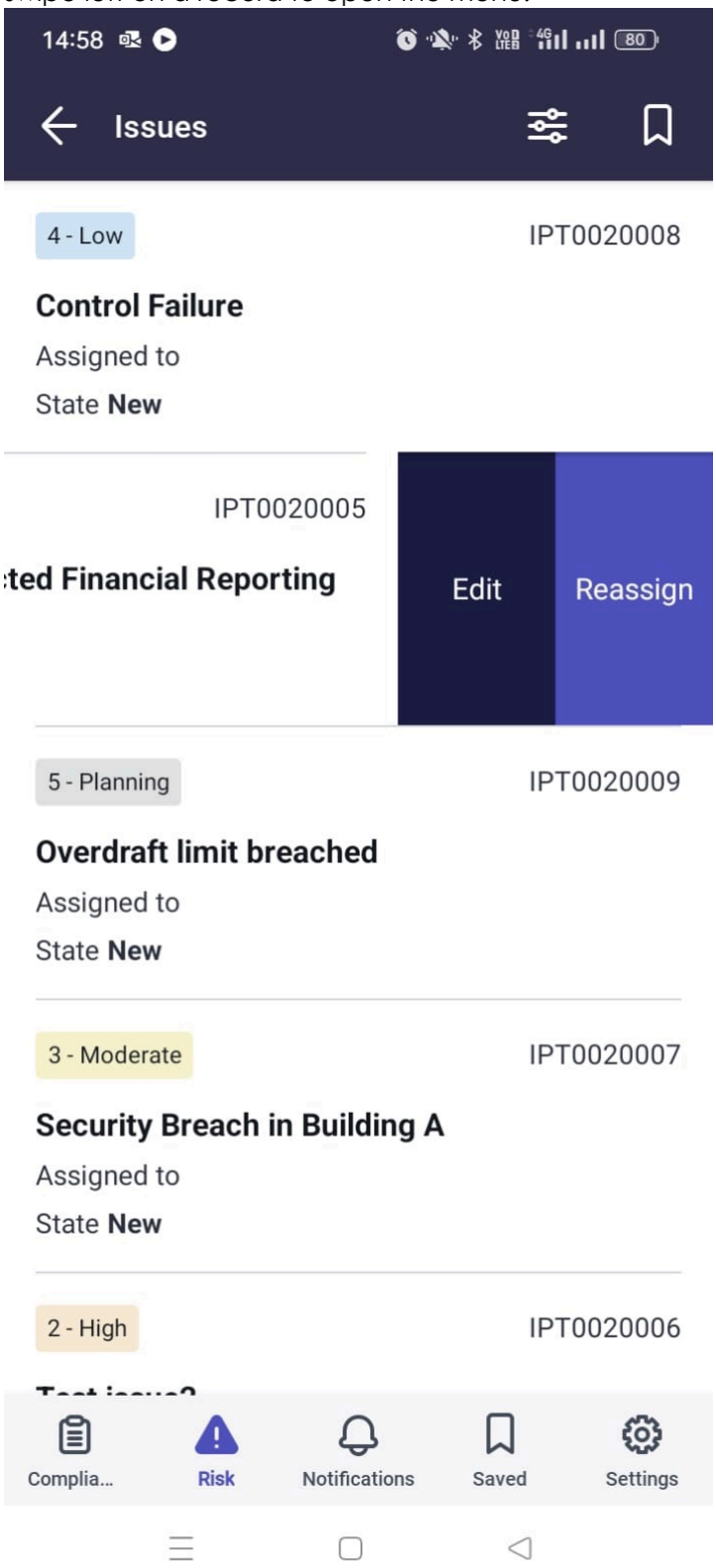



3. Optional: See Filter records with the GRC Mobile application to search for records that match specific search criteria.

   (Optional) Filtering records on screens in the mobile app works like filtering with a condition builder on the Now Platform. Setting filters can reduce the number of records that are displayed on screens.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To edit or reassign a task directly from the list of records displayed on the Issues screen, swipe left on a record to open the menu.




5. In the menu that is displayed, choose one to continue.

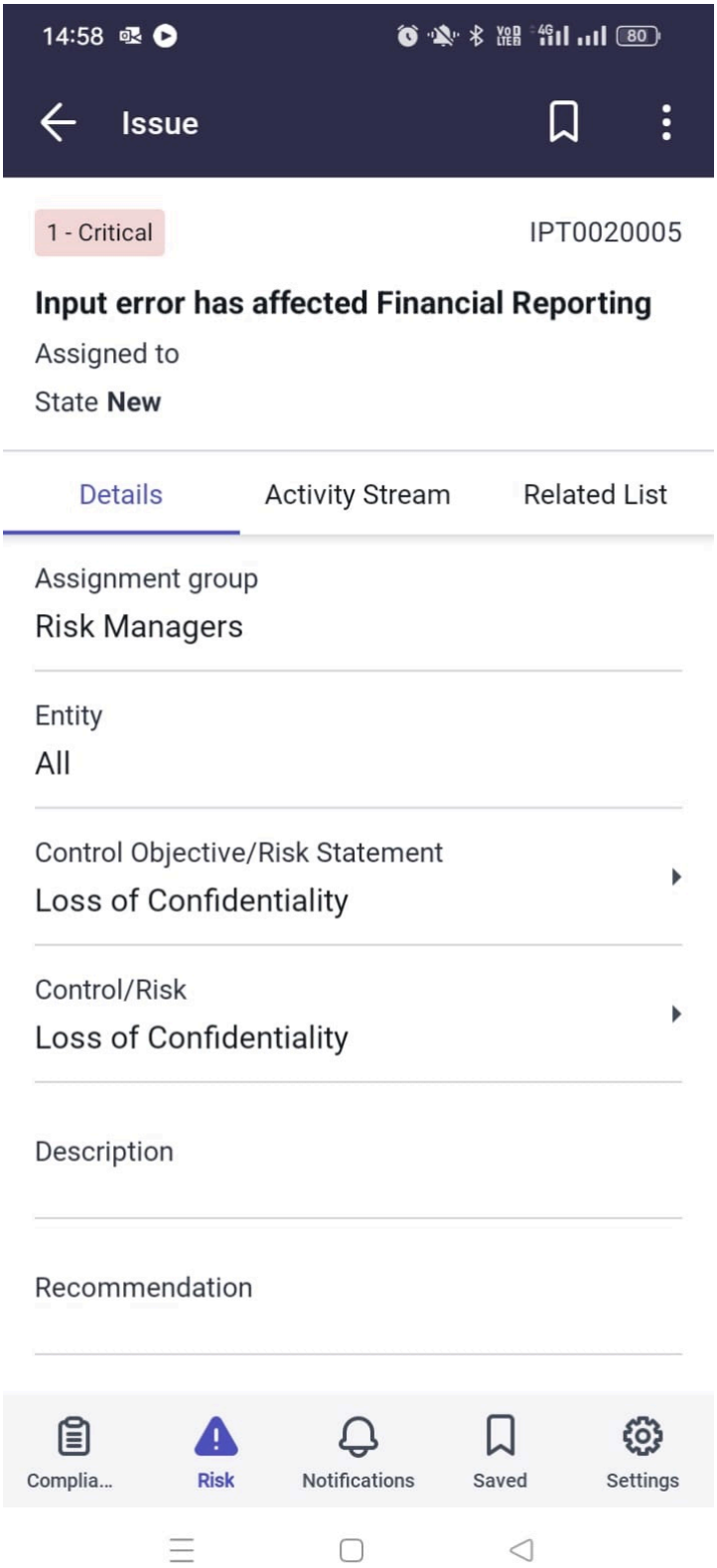
| Option | Description |
| --- | --- |
| Edit | In the Extend by days field on the Edit Issue screen that is displayed, enter a value. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | This value is added to the Duration field in your Now Platform instance. Tap the Send icon ( ) or **Submit** to save and submit your changes. |
| Reassign | On the Issue Assignment screen that is displayed, tap the Assignment Group and Assigned to fields to reassign the issue. Tap the Send icon ( ) or **Submit** to save and submit your changes. |

6. Alternatively, with the Issues screen displayed, tap a record on the list to open it and view more details.
7. With the fields on the issue record displayed, choose one in the following table to continue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




| Option | Description |
| --- | --- |
| Details tab | With the Details tab selected, choose one to continue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | ◦ View the fields for details about the issue, especially the planned start and end dates.<br><br>Tap the **Control Objective/Risk Statement** field to expand it. A list of records is displayed. Tap an item to display the record.<br><br>◦ Tap the **Control/Risk** field to expand it. A list of records is displayed. Tap an item on the list to open the record. With the record displayed, select the **Details** or **Activity Stream** tabs for more information.<br><br>◦ At the top right of the screen with the Issue record displayed, tap the menu icon ( ) to edit and reassign the issue. Follow the steps described in the preceding table. |
| Activity Stream tab | With the Activity Stream tab selected, choose one to continue.<br><br>◦ View work notes and additional comments. Tap the plus icon ( ) to add a work note or attach a file.<br><br>◦ At the top right of the screen, tap the menu icon ( ) to edit and reassign the issue. Follow the steps described in the preceding table. |
| Tap the Related List tab. | With the Related List tab selected, follow these steps.<br><br>**a.** Tap **Remediation Tasks** to expand the field. On the Remediation Task screen, view the items on the related list that are associated with the Issue record. Tap an item to open a record and view details and work notes.<br><br>**b.** After your review, navigate back to the open record on the Issue screen and tap the menu icon ( ) to reassign or edit the issue. Follow the steps described in the preceding table. |
| Tap a screen icon at the bottom of the screen. | On the bottom of the screen, choose one to continue.<br><br>◦ Tap the Risk icon to return the landing screen.<br><br>◦ If displayed, tap an icon to open another ServiceNow® mobile app.<br><br>◦ Tap **More**: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | ▪ Tap **Notification** to view notifications from the Now Platform and the GRC Mobile application.<br>▪ Tap **More** followed by **Settings**. Tap **Log out** to log out of the current instance. |

### Filter records with the GRC Mobile application

Set additional filters to limit the number of records that are displayed on a screen. Filtering records in the mobile app works like filtering with a condition builder on the Now Platform.

#### Before you begin
Role required: admin

#### About this task
Time to complete this task: 5 minutes.

#### Procedure
1. To further refine your search results, or to enter additional filter criteria on any list of records that is displayed, tap the filter icon (  ).
2. With the Filters screen displayed, tap a field to expand it.
3. From the options that are displayed, tap the check box or tap an item for your filter. For many of the filters, you can select more than one option.
4. Tap the Back icon (  ) or **DONE** to save your changes to a field. The criteria you chose are displayed on the Filters screen. The number of records that match your criteria is also displayed at the top of the screen. Tap **Clear** or **RESET** to remove any filters and restore the default setting.
5. Optional: Repeat steps 1 - 4 with the Filters screen displayed to continue setting your filter criteria.
6. Tap the intersection icon after you set all criteria to create AND conditions.  ). Alternatively, tap the union icon (  ) to create OR conditions.
7. After you have added all the criteria you want, with the Filters screen displayed, tap **DONE**. On the screen, only the records that match your filter criteria are displayed.

#### What to do next
View the records that are displayed after your search for more details.

## Use Risk Events

Report risk events and monitor their workflow to prevent losses in your organization.

### Configure risk event integration

Configure risk event integration with other upstream ServiceNow applications. This integration enables all users in an organization to report and track the risk events.

#### Before you begin
Role required: sn_risk.admin and user_admin

#### About this task
When you configure the risk event integration with another upstream application, then users of that application can directly report risk events from the application. For example, if you

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

configure risk event integration in the ServiceNow® IT Service Management (ITSM application, all users of ITSM can report risk events from the ITSM application. By default, this configuration is provided for the IT Incidents application and the Security incidents application.

The two modes that enable the creation of a risk event are **Simple** and **Advanced**. The **Simple** mode enables you to define filter conditions on the application table so that users of the Incidents application can report a risk event. For example, you can define that a financial event with a high impact must be reported as a risk event. In contrast, the **Advanced** mode enables users with GRC developer role to write scripts.

Incident managers with the incident_manager role are able to see the **Report Risk Event** option in an incident, whereas Security Managers with the sn_si.manager role are able to see the **Report Risk Event** option in a security incident.

### Procedure

1. Navigate to **Risk Events** > **Administration** > **Integration Configuration**.
2. Click **New**.
3. On the form, fill in the fields.

**Risk Event Integration Configuration form**

| Field | Description |
|---|---|
| Number | Configuration number. This field is automatically set. |
| Active | Option to enable the creation of a risk event from the application table. |
| Integration name | Short and unique title for the integration. For example, to report a risk event from an incident table, you can type `Incident-risk-event-integration`. |
| Application table | Application table that is used for reporting risk events. The table determines the upstream application that will be used for reporting risk events. |
| Source for name | How the name of risk events are set. The choices are as follows:<br>◦ **Form field**: Select this option if you want the value from a specific selected field to be used as the risk event name.<br>◦ **Default value**: Enter a custom value. The risk event is created with the name you enter here. |
| Source for description | How the description of risk events are set. |
| Source for entity | How the entity of risk events are set. |
| Source for date of discovery | How the date of discovery for risk events are set. |
| Name | Field in the application table that is used to set the name of risk events. This field appears only when **Form field** is selected from the **Source of name** field. |
| Default Name | Default name for risk events. This field appears only when **Default value** is selected from the **Source of name** field. |
| Description | Field in the application table that is used to set the description of risk events. This field appears only when **Form field** is selected from the **Source of description** field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Default description | Default description for risk events. This field appears only when the **Default value** is selected from the **Source of description** field. |
| Entity | Field from the application table that refers to a GRC entity or to a record in a GRC entity. This field appears only when **Form field** is selected from the **Source of entity** field. |
| Default Entity | Default entity for risk events. Default entities are created from the table in the **Application table** field. This field appears only when **Default value** is selected from the **Source of entity** field. |
| Date of discovery | Field in the application table that is used to set the date of discovery of risk events. This field is visible only when **Form field** is selected from the **Source of date of discovery** field. |
| Default date of discovery | Default date of discovery of risk events. |
| Default event type | Default event type of risk events. For example, if the event is financial or non-financial. |
| Event subtype | Subtype of the risk event. For example, if the event is actual or potential. |
| Source for Non-Financial impact | How the non-financial impact of risk events is set. |
| Non-Financial impact | Field in the application table that is used to set the non-financial impact of risk events. This field appears only when **Form field** is selected from the **Source of non-financial field** field. |
| Default non-financial impact | Default severity of risk events. The choices are **Low**, **Medium**, or **High**. |
| Source for expected loss | How the expected loss of risks events is set. |
| Expected loss | Field in the application table that is used to set the expected loss of risk events. This field appears only when **Financial impact** is selected from the **Default event type** is field and only when **Form field** is selected from the **Source of expected loss** field. |
| Default expected loss | Default monetary value of the loss. This field appears only when the **Financial impact** is selected from the **Default event type** field and only when **Default value** is selected from the **Source of expected loss** field. |
| Display UI Action Based On | |
| Mode | Mode that is used to create the UI action. The choices are as follows:<br>◦ **Simple**: Mode to set simple filter conditions. For example, if the impact of an incident is **High**, the **Report a Risk Event** UI action must be created.<br>◦ **Advanced**: Mode to write a script to query tables, including the table from the **Application table** field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Role condition | Roles that can report risk events from the upstream application. |
| Filter condition | Build the filters as per the requirement. |
| Script | Field to write a custom script to query any table.<br>**Note:** The option to write a script is only available to users who also have the sn_grc.developer role. This field appears when the **Mode** field has **Advanced**. |

4. Click **Submit**.
   Any other application table which extends the task table can configure this integration. For details, see the Risk Event Ingestion [KB0780985] article in the Now Support Knowledge Base. You must log in to view the article.

### Result
The application that is configured to report risk events displays the **Create Risk Event** button.

## Create a risk event response template

Automatically add approvers, issues, and owners to a risk event based on the conditions defined in the risk event response template.

### Before you begin
Role required: sn_risk.manager and sn_risk.admin

### Procedure
1. Navigate to **All** > **Risk Events** > **Administration** > **Response Templates**.
2. Click **New**.
3. On the form, fill in the fields.

#### Risk Event Response Templates form

| Field | Description |
|---|---|
| Number | Template number. This number is automatically set. |
| Entity | Entity that the template is created for. |
| Category | Category that the risk event applies to if there is an occurrence. You can edit the category to apply one of the following options.<br>◦ **Personal**: For example, any physical harm caused to an employee.<br>◦ **Legal**: For example, an employee conducts a business that is a conflict of interest.<br>◦ **Information Security**: For example, a theft, burglary, or system crash. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ **Human Resources**: For example, sensitive lawsuits by an employee against another employee.<br>◦ **All**: Any risk event that is reported. |
| Approval rule based on | Rule used while assigning the event.<br>◦ **Gross Loss**<br>◦ **Net Loss**<br>◦ **Expected Loss**<br>This field depends on the values in the **Event type** and **Sub type** fields. For example, if the event type is **Financia**l, and the sub type is **Actual**, the approval rule is based on gross loss, net loss, or expected loss. If the Sub type is **Potential**, the approval rule is expected loss, by default. If the Event type is **Non-Financial Impact**, the approval rule is Non-financial, by default. |
| Event type | Event type.<br>◦ **Financial Impact**: Indicates that the event has an associated financial loss. Enter the amount. You can choose the currency.<br>◦ **Non-Financial Impact**: Indicates that while the event does not have any financial loss, it does have a non-financial impact on the organization. For example, non-financial impact can be negative market news or a decline in employee morale. |
| Sub type | Event sub type. Select one of the following:<br>◦ **Actual**<br>◦ **Potential** |
| Auto close event once approved | Option to select if the event must be closed after approval. Selecting this option results in closing of the event after the issue and root cause are closed. If a risk event has open issues or tasks, the risk event is not closed even after approval. |

4. In the Risk Event Owner Assignment section, select the assignment type and the owner or owning group.
5. To automatically create an issue, select the **Automatically create issue** check box in the Issue Creation and Assignment section.
6. In the Root Cause Analysis Task section, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk Event Response Templates form**

| Field | Description |
|---|---|
| Automatically create RCA task | Task creation for root cause analysis (RCA). Automatically create a Root Cause Analysis (RCA) task based on the amount entered in the **Threshold for task creation** field. |
| Assigned to | Person that the RCA task is assigned to. |
| Threshold for task creation | Option to specify the threshold amount after which an RCA task is created. For example, users can specify that after an event crosses loss worth $1000, an RCA task must be created. |
| Priority | Priority of the event. Select from:<br>◦ **Critical**<br>◦ **High**<br>◦ **Moderate**<br>◦ **Low**<br>◦ **Minor** |

7. Click **Submit**.
   A new risk event response template is created.

### Define a threshold amount for the risk event response template

Define a threshold limit for assigning risk event approvers. A threshold limit is defined to determine if a risk event needs an approver.

#### Before you begin

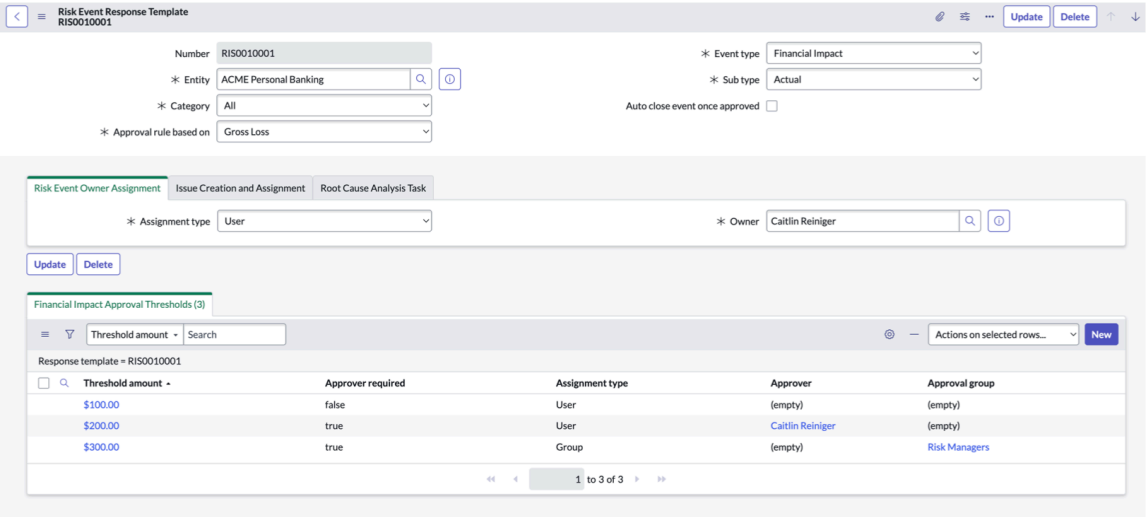
Role required: sn_risk.manager and sn_risk.admin

#### About this task

Based on the risk loss amount, you can decide whether approvers are required for the risk events losses. For example, for any risk event that results in a loss of $1000 or less, an approver is not needed. But for any amount beyond $1000, the risk event must be evaluated and an approver is automatically assigned. There can be multiple levels of approvals

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

depending on your defined thresholds. For a better understanding, see the following image.




In the previous example, the following rules are applied.

- If the loss is between $0-$100, approval is not required.
- If the loss is between $101 – $200, approval is required and approval goes to Caitlin.
- If the loss is over $201 approval will be required from both Caitlin and the Risk manager.

## Procedure

1. Navigate to **All** > **Risk Events** > **Administration** > **Response Templates**.
2. Select and open the risk event response template for which you want to add the financial threshold limit.
3. In the Financial Impact Approval Thresholds related list, click **New**.
4. From the **Threshold amount** list, select the currency type and enter the amount that needs an approval.
5. Select the **Approver required** check box.
6. From the **Assignment type** list, select either **User** or **Group**.
7. In the **Approver** field, select the approver to approve the risk event if the threshold amount is exceeded.
8. Click **Submit**.

## Result

The response template is updated with the threshold limit and approver details.

### Report risk events from the Service Portal

When you identify any event that might have a financial or non financial impact on your organization, report it from the ServiceNow, Inc. Service Portal. You can also report any event that has already occurred with a financial or non financial impact.

## Before you begin

Role required: ServiceNow user

## About this task

You can log your risk event under any of the following event types:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Risk event with financial impact
- Risk event with non-financial impact

### Procedure

1. In the Service Portal, click **Catalog** > **Browse by Categories**.
2. Click **Governance Risk and Compliance** and then click **Report Risk Event**.
3. On the form, fill in the following fields:

**Report risk event**

| Field | Description |
|---|---|
| Title | Enter the title of the risk event reported. |
| Description | Enter the description of the risk event reported. |
| Show my entities only | When selected, only the entities owned by you are displayed. This value is taken from the **Owner** field on the **Entity** form. By default, this option is selected. |
| Entity where the event occurred | Select the entity that will absorb or report the loss. Select only one entity from the list. |
| Other entities affected | Select other related entities that are affected by the event.<br>**Note:** You can select more than one entity. |
| Event type | Select one of the following:<br>◦ Financial Impact- This indicates that the event has an associated financial loss. Enter the amount in your local currency.<br>◦ Non-financial Impact- This indicates that while the event does not have any financial loss, it does have a non-financial impact on the organization. For example, a non-financial impact can be negative market news or a decline in employee morale. |
| Currency | Select the currency for the loss. This field appears only when the event type is Financial. |
| Date of discovery | Select the date when the risk event was discovered. |
| How was the event discovered | Select how the event was discovered. For example, if the risk event was reported by a customer, select **Customer Feedback/Complaint**. |
| Root cause | Enter your analysis for the cause of the event. For example, if a fire occurs in a server room, the root cause may be an increase in temperature or an electrical short circuit. |
| Action taken | Enter what was done to reduce the impact of this risk event. For example, if the fire in the server room was caused by an electrical short circuit, then the action taken is a replacement of the defective equipment. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Click **Submit**.
5. To view all the risk events you have reported, navigate to **GRC > My Risk Events**.

### Result

The risk event is created in the system and is ready to be analyzed by the risk manager. When an action is taken on the event, you will receive notifications on the status. You can respond to queries or track the status of the event during its life cycle.

#### Report a risk event from Employee Center

When you identify any event that might have a financial or non financial impact on your organization, report it from the ServiceNow, Inc. Employee Center. You can also report any event that has already occurred with a financial or non financial impact.

### Before you begin

Role required: sn_grc.business_user, or sn_grc.business_user_lite

### Procedure

1. Navigate to **All** > **Self-Service** > **Employee Center**.
2. Select **Risk & Compliance**.
3. Select **Report Risk Event**.
4. On the form, fill in the fields.

#### Report risk event form

| Field | Description |
|---|---|
| What was the event? | Brief description of the event. |
| Describe in detail what happened | Detailed description of the event. |
| Show my entities only | When selected, only the entities owned by you are displayed. This value is taken from the **Owner** field on the **Entity** form. By default, this option is selected. |
| Which entity is impacted by this event? | The entity that will absorb or report the loss. |
| Other entities affected | Select other related entities that are affected by the event.<br>**Note:** You can select more than one entity. |
| What kind of impact will this event have? | Type of impact. The choices areas follows:<br>◦ Financial Impact- This indicates that the event has an associated financial loss.<br>◦ Non-financial Impact- This indicates that while the event does not have any financial loss, it does have a non-financial impact on the organization. For example, a non-financial impact can be negative market news or a decline in employee morale. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Currency | Currency for the loss. This field appears only when the event type is set to **Financial Impact**. |
| How much financial loss this event may cause? | Loss amount due to the event. This field appears only when the event type is set to **Financial Impact**. |
| How would you rate the non-financial impact of this event? | Non-monetary impact of the event. The choices are as follows:<br>◦ **Low**<br>◦ **Medium**<br>◦ **High** |
| When did you discover the event? | Date the event was discovered. |
| How was the event discovered? | How the event was discovered. For example, if the risk event was reported by a customer, select **Customer Feedback/ Complaint**. |
| What do you think caused this event? | Provide your analysis for the cause of the event. For example, if a fire occurs in a server room, the root cause may be an increase in temperature or an electrical short circuit. |
| What actions have been taken so far to contain this event? | Provide the actions taken to reduce the impact of this risk event. For example, if the fire in the server room was caused by an electrical short circuit, then the action taken is a replacement of the defective equipment. |

5. Select **Submit**.

### Result
The risk event is submitted for review.

#### Report a risk event from an incident

If risk event integration is configured, users can report risk events from any upstream application such as IT Incidents. This ability to report risk events saves the time of users and helps to prevent losses for organizations.

### Before you begin
Role required: sn_risk.user

### Procedure

1. Navigate to **All** > **Incident** > **All**.
2. Open the incident for which you want to report a risk event.
3. Select **Report Risk Event**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The availability of the **Report Risk Event** button on the incident record is determined by the filter conditions specified in the Risk Event Integration Configuration record. For more information, see Configure risk event integration.

4. On the form, fill in the fields.

**Report Risk Event form**

| Field | Description |
|---|---|
| Name | Name of the incident. |
| Date of discovery | The date the incident was created. |
| Entity | The entity to which the incident belongs. |
| Event type | Type of event. The choices are:<br>◦ Financial impact<br>◦ Non financial impact |
| Currency | Currency in which the amount of loss is reported. This field appears if **Financial impact** is selected from **Event type**. |
| Expected Loss | Expected amount of monetary loss. This field appears if **Financial impact** is selected from **Event type** |
| Non Financial Impact | Impact of the incident. The choices are:<br>◦ Low<br>◦ Medium<br>◦ High |
| Description | A brief description of the incident. |

5. Select **Submit**.

### Result
The risk event is created.

## Create a risk event task

A risk event might require associated tasks. Unless these tasks are created and eventually closed, the risk event cannot be closed.

### Before you begin
Role required: sn_risk.manager

### Procedure

1. Navigate to **All** > **Risk Events** > **All Events**.
2. Select the record for which a task must be created.
3. Select the Tasks related list and then select **New**.
4. On the form, fill the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

#### Risk event task form

| Field | Description |
|---|---|
| Assigned to | Person that the task is assigned to. |
| Priority | Level of importance given to a task, which indicates how readily a task or assignment can be delayed. |
| Short description | Brief description of the task. |
| Description | Detailed description of the task. |
| Work notes | Any relevant information for your reference. |
| Additional comments | Any additional information that might be necessary. |

5. Select **Submit**.

### What to do next
Review the associated issues of a risk event or create a new issue during approval. For more information, see Manually create GRC issues.

## Analyze a risk event

Analyze user-submitted risk events to determine if the risk event is valid and needs further processing.

### Before you begin
Role required: sn_risk.manager

### About this task
When you analyse a risk event, you add more relevant details to the risk event that is submitted. During analysis, you can either reject the event if the risk event doesn't appear to be an actual risk event, or request more information if the information is insufficient.

### Procedure
1. Navigate to **All** > **Risk Events** > **All Events** and open the risk event that you want to analyze. Alternatively, you can also navigate to **Risk Events** > **New Events**.
2. On the form, review the fields and edit them as necessary.

#### Risk event form

| Field | Description |
|---|---|
| Name | Name of the risk event. Edit the name of the risk, if necessary, to provide a more intuitive name. |
| Number | Number of the risk event. This field is automatically set. |
| Discovered by | The person who discovered the risk event. Edit the **Discovered by** field, if necessary. |
| Opened by | Person who created the event. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Primary entity | Entity that bears the loss. This entity is visible to management for reporting. |
| Owning group | Group responsible for monitoring the event to closure. |
| Owner | The person who owns the risk event. A risk manager can be an event owner. If the owning group is specified, the owners are filtered from the owning group. |
| State | State of the risk event. This field is automatically set. |
| Substate | Substate of the event. This field is automatically set. |
| Event type | Type of event. You can edit the event type, if necessary. For example, if during analysis you observe that the event type isn't a financial impact, you can edit the entry. |
| Sub type | Event sub type. You can edit the sub type, if necessary. For example, if during analysis you observe that the event type isn't an actual event but a potential event, you can edit the entry. |
| Category | Event category. You can edit the category to apply one of the following options:<br>◦ **Personal**: For example, any physical harm caused to an employee.<br>◦ **Legal**: For example, an employee is found conducting business that is a conflict of interest.<br>◦ **Information Security**: For example, a theft, burglary, or system crash.<br>◦ **Human Resources**: For example, sensitive lawsuits by an employee against another employee. |
| Approvers | The person who approves the risk event. Any user with the sn_risk.user role can approve the risk event. |
| Cost center | Corresponding account number of the entity. |
| Description | Detailed description of the event in this field. |
| Dates | |
| Date of occurrence | Exact day, month, and year when the event occurred. For example, a mortgage was lent against a property that didn't comply with the building regulations on August 12, 2019. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Date of discovery | Date that the event was first discovered or noticed. For example, the mortgage was discovered on August 24, 2019. |
| Date of first recognition | Date that the event was first recognized and entered in the book of accounts. For example, the loss entries were entered in the firm's book of accounts on August 26, 2019. |
| Loss/Gain Estimates | |
| Expected loss | Amount of loss expected. Expected loss is the probability weighted average of all possible losses. This amount is based on the user's judgment of the expected amount that the organization might lose. |
| Potential loss | Amount expected to be a potential loss due to the risk event. This amount is the maximum loss an entity can incur due to the loss from the risk event. |
| Event Analysis | |
| Cause | Primary reason why the risk event occurred. |
| Cause description | Brief description about why the risk event occurred. |
| Consequence | Consequence of the risk event. For example: Regulatory fines can be imposed as a result of the risk event. |
| Actions taken | Remedial actions that were taken to address the issue. This is the initial record of the event. |
| Credit/Market Risk | |
| Boundary event | Option for a boundary event. A boundary event is an operational risk event which leads to a consequence, such as a financial loss in another risk category. |
| External risk type | ◦ **Credit**: Credit risk is the possibility of a loss resulting from a borrower's failure to repay a loan or meet contractual obligations. For example, when lenders offer credit cards, or loans, there's a risk that the borrower might not repay the loan.<br>◦ **Market**: Market risk is the possibility of an investor incurring losses due to factors that affect the performance of the financial markets in which the investor is involved. For example, a recession might impact the entire market. |
| External risk reference | ID for reconciliation in the book of accounts. Specify the IDs for reconciliation |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | purposes. The credit and market risk systems are different. |
| Additional Classification | |
| Used in modeling | Option to share these risk event records with external systems where they want to perform advanced analysis using simulation techniques such as Monte Carlo simulation. |
| Full rapid recovery | Total loss recovered. Select if the total loss is recovered within a short duration and doesn't impact the organization.<br>**Note:** Generally, a short duration refers to five working days, but this value can be configured according to your requirements. |
| Financial gain | This option is automatically selected if the risk event meets one of the following conditions.<br>◦ Risk event is a potential event and the **Expected loss** field or the **Potential loss** field has a negative value because of the gain.<br>◦ Risk event is an actual event and the **Net loss** field has a negative value. |
| Near miss | This option can either be modified or can be automatically set based on the event type. If the event sub type is **Actual**, and the **Full rapid recovery** option is selected, the **Near miss** option is automatically selected. |
| Reason for near miss | Reason which prevented the risk event from incurring the loss. If the event type is Potential, select the **Near miss** option and in the **Reason for near miss** field, enter the reason why the event was a near miss |
| Confidentiality | |
| **Note:** This section only appears when:<br>◦ The *sn_grc.enable_record_confidentiality* property is enabled under GRC properties.<br>◦ The risk event is in New or Analyze state | |
| Confidential | Option to mark the risk event record as confidential. |
| Allowed users | Users who can view the risk event. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** By default, the risk event owner and the logged in user are added to the list of confidential users. |
| Allowed groups | Groups that can view the risk event. |
| Summary | |
| To understand how the values in this section appear, refer to the example given after this step. | |
| Direct amount | The aggregated sum of all direct losses. This field is automatically set. |
| Additional cost | The aggregated sum of all additional costs. This field is automatically set. |
| Gross loss | Sum of all direct losses, indirect amounts, and additional costs. This field is automatically set. |
| Net loss | The net amount of the loss. This field is automatically set. |
| Indirect amount | The aggregated sum of all indirect losses. This field is automatically set. |
| Rapid recovery amount | The aggregated sum of the amount that was recovered rapidly. This field is automatically set. |
| Recovered amount | The amount to be recovered for the risk event. This field is automatically set. |
| Non financial impact | Impact of the event when it does not have a monetary loss. The choices are as follows:<br>◦ **None**<br>◦ **Low**<br>◦ **Medium**<br>◦ **High** |
| Activity | |
| Additional comments | Provide additional comments that you may have about the risk event. |
| Work notes | Option to provide work notes for reference. Work notes are not visible to the risk event creator. |

**Example**

The values in the Summary section, the values in the fields are calculated in the Event Impacts related list. For example, consider that a firm has a fire outbreak. This event can result in multiple direct and indirect impacts such as loss of information and business.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If you enter the value of a direct impact as **$2000**, then the **Direct amount** field reflects the same value. If you enter two indirect amounts, each with a value of **$300** and **$500** respectively, then the **Indirect amount** field reflects a value of **$800**.

If an external agency is hired to address the root cause of the fire outbreak, the cost incurred reflects an additional cost.

If the firm was able to recover a part of the cost of the event in five working days, then the **Rapid recovery amount** field reflects the same amount.

The **Gross loss** field reflects the total loss incurred by the event.

The currency conversion rates impact the values displayed in the Summary related list. For example, if you enter a value of **300** Japanese Yen as the recovery amount, you see the amount in the concurrent USD value of **2756** in the Summary related list. This conversion occurs because the currency conversion rates are applied from the Exchange Rate table. For more information on how the values in the exchange rate table are calculated, see Use your own currency-conversion rates.

3. To send the risk event for approval, click **Request Approval**.

### Create a risk event entry

Create a risk event entry to determine the monetary or non-monetary impact of the risk event. A risk event can have multiple risk event entries.

#### Before you begin
Role required: sn_risk.manager

#### About this task
Risk event entries capture the direct and indirect losses reported due to the risk event.

#### Procedure
1. Navigate to **All** > **Risk Events** > **All Events** and select the event to be analyzed.
2. Click the Risk Event Entries related list.
3. Click **New**.
4. On the form, fill in the fields.

**Event Entry form**

| Field | Description |
|---|---|
| Number | Number for the event entry. This field value is automatically set. |
| Risk event | Title of the risk event. This field value is automatically set. |
| Date of impact | Date that the impact was recorded.<br>**Note:** The date of discovery and the date of first recognition can be different. This date cannot be a future date. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Amount | Amount that the impact costs. The amount entered is reflected in the Summary related list. |
| Rapid recovery | Loss amount for this entry if it's recovered in a short time, which is generally five working days. |
| Impact type | Type of financial impact for the event. Select from the following types:<br>◦ **Direct/Indirect Impact**: Direct or indirect financial impact of the event on the entity.<br>◦ **Recovery**: Amount recovered from the total financial impact.<br>◦ **Additional Cost**: The additional cost incurred due to the impact.<br>◦ **Non-Financial Impact**: The event has no financial impact. |
| Category | **Direct** or **Indirect**. For example, if the impact is direct, is it external? |
| Sub category | Sub category of the event impact. Select one of the following categories:<br>◦ **External Cost**: The cost that's incurred for external agencies. For example, if a loss is incurred due to erroneous accounting and an external auditor was hired to assess the event, the cost incurred in employing the auditor is an external cost.<br>◦ **General Ledger**: The book of accounts in which this event is entered.<br>◦ **Booked Provision**: Refers to the amount that you set aside in your accounts to cover a future event. For example, if a firm sets aside an amount to cover a risk event that might occur in the future.<br>◦ **Revenue Reversal/Timing Losses**: When you reverse revenue, a reverse entry is created that backs out the original entry. Don't enter any new accounting information into the system. |
| GL account reference | Account number in which this entry is captured in the ERP system. |
| Short description | Brief description of the impact. |

5. Click **Submit**.

### What to do next

Create or edit a new risk

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Creating or editing a new risk for an event is useful for future prediction of risks. The information obtained from the risks is useful for scoring and reporting. For more information, see Create a risk manually.

Link new control to risks

A control is used to prevent a risk from occurring. Linking the controls to risks lets users know which controls failed and why the risk event occurred. This information can be used for future predictions and reporting.

**Note:** Only those risks and controls that are tagged to the impacted entity can be related to this risk event.

For more information, see Create a control.

### Approve a risk event

A user with the sn_risk.manager role must approve a valid risk event. If any risk approver rejects the event, the state of the risk event changes to rejected.

#### Before you begin
Role required: sn_risk.manager

#### Procedure

1. Navigate to **All** > **My Approvals**.
2. Click the record in the list with your name as the approver.
3. Click **Approve**.

### Close a risk event

Close a risk event to complete the risk events life cycle. A user with the sn_risk.manager role must close the risk event after verifying that all associated open issues and remedial tasks are closed.

#### Before you begin
Role required: sn_risk.manager

#### Procedure

1. Navigate to **All** > **Risk Events** > **Assigned to Me**.
2. Open the record that you want to close and verify if all the associated tasks and issues are closed.
3. Click **Close**.

### Add a risk event cause to the cause library

A cause library is a centralized library of the possible causes that can lead to a risk event. Adding causes helps to identify the reason for a risk event and prevent future events.

#### Before you begin
Role required: sn_risk.manager and sn_risk.admin

#### About this task
Add a risk event cause to the cause library to help with risk analysis, risk prediction, and risk prevention.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Risk Events** > **Administration** > **Causes**.
2. Click **New**.
3. On the form, fill in the fields.

#### Cause form

| Field | Description |
|---|---|
| Name | Name of the cause. For example, `Inadequate IT security`. |
| Parent | Parent of the cause. The parent refers to the group under which the cause is categorized. For example, for Inadequate IT security, the parent cause can be Process. |
| Description | Brief description of the cause. |

4. Click **Submit**.

### Result
The risk event cause is added to the library.

Related topics

Add a risk event consequence to the consequence library

## Add a risk event consequence to the consequence library

A consequences library is a centralized library of the possible consequences of a risk event.

### Before you begin
Role required: sn_risk.manager and sn_risk.admin

### About this task
Add a risk event consequence to the consequence library to help with risk analysis, risk prediction, and risk prevention.

### Procedure

1. Navigate to **All** > **Risk Events** > **Administration** > **Consequences**.
2. Click **New**.
3. On the form, fill in the fields.

#### Consequence form

| Field | Description |
|---|---|
| Name | Consequence name. For example, `Asset loss`. |
| Parent | Parent of the consequence. The parent refers to the group under which the consequence is categorized. For example, for Asset loss, the parent consequence can be Damage to Physical Assets. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Description | Brief description of the consequence. |

4. Click **Submit**.

### Result
The risk event consequence is added to the library.

Related topics

Add a risk event cause to the cause library

#### Set up GRC Virtual Agent to report risk events

Use a Virtual Agent chatbot to report risk events from the Service Portal. A virtual agent chatbot helps customers to quickly report a risk event. The chatbot assists the customers by saving their time. The information exchanged during the conversation flow enables the chatbot to fulfill a user request or assist the user in completing a task.

### Before you begin
Customers must have the following plugins activated for setting up the GRC Virtual Agent

- Glide Virtual agent (com.glide.cs.chatbot) activated with a valid license.
- GRC Advanced Risk.

Role required: sn_risk.admin.

### Procedure

1. Navigate to **All** > **Service Portal** > **Service Portal Configuration**.
2. Click **Page Editor**.
3. In the search field, enter `Index`.
4. Click **Service Portal index**.
5. At the top of the page, click **Edit Service Portal (index) page in Designer**.
6. In the Filter Widget search field, type `Virtual Agent Service Portal Widget` , drag the widget, and drop it anywhere on the screen.

   You can see the chat icon at the bottom-right of the screen.

## Perform Advanced Risk Assessment

Use the ServiceNow® Governance, Risk, and Compliance (GRC) Advanced Risk Assessment feature to create an integrated risk platform.

To see the roles required for performing and approving the assessment, refer to Roles for performing advanced risk assessment.

#### Create a manual factor

Create manual factors to evaluate and assess risks on a risk assessment instance.

### Before you begin
Role required: sn_risk.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

Manual factors need human responses. You can create manual factors and associate them with various assessment types, such as an inherent assessment, control assessment, or residual assessment.

**Note:** You can only delete a factor if there are no Risk assessment methodologies (RAMs) associated with the factor.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Manual Factors**.
2. Select **New**.
3. On the form, fill in the fields.

#### Manual Factor form

| Field | Description |
|---|---|
| Name | Name of the factor such as `Reputational impact`. |
| State | State of the factor. This field is automatically set to **Draft**. |
| Factor contribution | Type of factor contribution. Choices are the following:<br>◦ **Qualitative**: Provides a numerical score and then converts the score into a rating.<br>◦ **Quantitative**: Provides the losses that can be incurred in monetary terms. The losses contribute to the annual loss expectancy (ALE).<br>◦ **Both**: Assessment type is both qualitative and quantitative. |
| Display order | Order of questions in the assessment form. This field enables you to set a specific sequence in which the questions must appear. |
| User response | Option for users to respond to the factors. Choices are the following:<br>◦ **Choice**: Users can create choices such as low, medium, and high alongside their respective scores.<br>**Note:** Selecting this option displays the Choices related list. Save the form to see the Choices related list.<br>◦ **Number**: Users can enter a number in response to a factor.<br>◦ **Text**: Users can enter text in response to a factor. This option does not contribute to the score, and it is used as guidance or as a data collection method. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ **Currency**: Users can enter currency in response to a factor.<br>◦ **Percentage**: Users can enter a percentage in response to a factor. |
| Control type | Option to modify the layout of factor choices on the risk assessment form. Choices are as follows:<br>◦ **Radio**: Displays the factor choices in radio buttons.<br>◦ **Drop-down**: Displays the factor choices in a drop-down list.<br>This field appears only when **Choice** is selected from the **User response** field. |
| Control layout | Option to display the factor choices in vertical or horizontal layout.<br>This field appears only when **Radio** is selected from the **Control type** field. |
| Transform qualitative score | Option to transform the overall group qualitative score based on an interval scale.<br>For example, assume the **User response** field is set to **Percentage**. As the admin, you can transform the percentage value into a qualitative score, such that 0% to 30% is low, 30% to 60% is medium, and 60% and higher is high. In this case, the ratings 1, 2, and 3 can be assigned to low, medium, and high.<br>This field appears only when **Qualitative** is selected from the **Factor contribution** field. |
| Qualitative weighting (%) | Score contribution or qualitative weight that is given to the factor. This value determines the actual contribution of this factor to the final score. This value is a percentage. This field appears only when **Qualitative** is selected from the **Factor contribution** field. |
| Mandatory response | Option for making the responses mandatory. |
| Description | Brief description about the purpose of the factor and where to use the factor. This description is for the administrator to understand the factor. |
| Guidance text | Guidance on how to respond to the factor. If the risk assessor does not understand the factor's question, then this field can help |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | explain the question. For example, if the assessor wants to understand a question about the financial impact of losing a high value asset, the assessor can get guidance from this field. |

4. Click **Save**.
5. Click the Qualitative Transformation Criteria related list.

> **Note:** This related list appears only when you select the **Transform qualitative score** option.

6. On the form, fill in the fields.

**Qualitative Transformation Criteria form**

| Field | Description |
|---|---|
| Lower limit of range | Value that is the lower limit of a range of values. For example, for the first range of 0% to 30%, the lower limit is 0. For the second range of 31% to 60%, the lower range is 31. |
| Score | Value that must be used as the score if the value is within the range defined in the **Lower limit of range** field. For example, for the lower limit 0, the score can be 1. For the lower limit 31, the score can be 2. |

7. Click **Submit**.
8. Open the factor that you created.
9. Click **Publish**.

### Result
The factor is published and is ready for use in a Risk Assessment Methodology.

## Create a group factor

Create group factors to evaluate and assess risks on a risk assessment instance.

### Before you begin
Role required: sn_risk.admin

### About this task
Group factors contribute to either a numerical risk score or to the Annual Loss Expectancy (ALE). You can group multiple factor responses into one group factor that can be used for reporting. The score of a group factor is computed based on the scores of its associated factors.

### Procedure
1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Group Factors**.
2. Select **New**.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Group Factor form

| Field | Description |
|---|---|
| Name | Name of the factor such as `Organizational impact`. |
| Factor contribution | Type of factor contribution. Choices are the following:<br>◦ **Qualitative**: Provides a numerical score and then converts the score into a rating.<br>◦ **Quantitative**: Provides the losses that are incurred from a risk in monetary terms. The losses contribute to the ALE.<br>◦ **Both**: Assessment type is both qualitative and quantitative. |
| Display order | Order of questions in the assessment form. This field enables you to set a specific sequence in which the questions must appear. |
| State | State of the factor. This field is automatically set to **Default**. |
| Qualitative weighting (%) | Score contribution or qualitative weight that is given to the factor. This value determines the actual contribution of this factor to the final score. This value is a percentage. This field appears only when **Qualitative** is selected from the **Factor contribution** field. |
| Description | Brief description about the purpose of the factor and where to use the factor. This description is for the administrator to understand the factor. |
| Qualitative Score | |
| This section appears only when **Qualitative** is selected from the **Factor contribution** field. | |
| Formula for qualitative score | Formula for calculating the overall qualitative risk score. Choices are the following:<br>◦ **Sum**: Sum of the factor responses.<br>◦ **Minimum**: Minimum value of the factor responses.<br>◦ **Maximum**: Maximum value of the factor responses.<br>◦ **Average**: Average value of the factor responses.<br>◦ **Product**: Value derived by multiplying the factor responses. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ **Weighted average**: Average value of the weighting of factors.<br>◦ **Script**: User-defined formula to calculate the score. This option is available only to users with the sn_grc.developer role. |
| Transform qualitative score | Option to transform the overall group qualitative score based on an interval scale.<br><br>For example, assume the **User response** field is set to **Percentage**. As the admin, you can transform the percentage value into a qualitative score, such that 0% to 30% is low, 30% to 60% is medium, and 60% and higher is high. In this case, the ratings 1, 2, and 3 can be assigned to low, medium, and high.<br><br>This field appears only when **Qualitative** is selected from the **Factor contribution** field. |
| Quantitative Score | |
| This section appears only when **Quantitative** is selected from **Factor contribution** field. | |
| Formula for quantitative score | Formula for calculating the overall qualitative risk score. Choices are the following:<br>◦ **Sum**: Sum of the factor responses.<br>◦ **Minimum**: Minimum value of the factor responses.<br>◦ **Maximum**: Maximum value of the factor responses.<br>◦ **Average**: Average value of the factor responses.<br>◦ **Product**: Value derived by multiplying the factor responses.<br>◦ **Script**: User-defined formula to calculate the score. This option is available only to users with the sn_grc.developer role. |

4. Select **Save**.
5. In the Factors related list, click **Edit** and add the required factors.
6. Select **Save**.
7. Select the Qualitative Transformation Criteria related list.
8. On the form, fill in the fields:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

#### Qualitative Transformation Criteria form

| Field | Description |
|---|---|
| Lower limit of range | Value that is the lower limit of a range of values. For example, for the first range of 0% to 30%, the lower limit is 0. For the second range of 31% to 60%, the lower range is 31. |
| Score | Value that must be used as the score if the value is within the range defined in the **Lower limit of range** field. For example, for the lower limit 0, the score can be 1. For the lower limit 31, the score can be 2. |

9. Select **Submit.**
10. Open the factor that you created.
11. Select **Publish**.

**Result**
The factor is published and is ready for use in a Risk Assessment Methodology.

#### Scoring logic for predefined formulas for group factors

Group factors have multiple predefined formulae and each of them has a specific contribution to the scoring logic.

## Predefined formulae scoring logic

Users can select one of the following predefined formulae to calculate the scoring for group factors. The scores are contributed by scores of manual factors that comprise a group factor and have factor contribution as Qualitative or Quantitative, or Both.

The qualitative scores calculated using the predefined formulae are transformed using the transformation criteria if the **Transform qualitative score** option is selected for the group factor.

The qualitative scores calculated after transformation will be derived using the Qualitative weighting of the group factor. For example, if the calculated score is 10 and the Qualitative weighting is 50%, then the final score for group factor will be calculated as 10 x 0.5 = 5.

Sum

For Qualitative, this formula adds up the qualitative scores in an assessment instance. The scores are contributed by scores of manual factors that comprise a group factor and have factor contribution as either Quantitative or Both.

For Quantitative, this formula adds up the quantitative scores in an assessment instance. The scores are contributed by scores of manual factors that comprise a group factor and have factor contribution as either Quantitative or Both.

Minimum

For Qualitative, this formula takes the minimum of qualitative scores in an assessment instance. The scores are contributed by scores of manual factors that comprise a group factor and have factor contribution as either Quantitative or Both.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For Quantitative, this formula takes the minimum of quantitative scores in an assessment instance. The scores are contributed by scores corresponding to the factors that a comprise a group factor and have factor contribution of either Quantitative or Both.

Maximum

For Qualitative, this formula takes the maximum of qualitative scores in an assessment instance. The scores are contributed by scores corresponding to the factors that a comprise a group factor and have factor contribution of either Qualitative or Both.

For Quantitative, this formula takes the maximum of quantitative scores in an assessment instance. The scores are contributed by scores corresponding to the factors that a comprise a group factor and have factor contribution of either Quantitative or Both.

Average

For Qualitative, this formula takes the average of qualitative scores in an assessment instance. The scores are contributed by scores corresponding to the factors that a comprise a group factor and have factor contribution of either Qualitative or Both.

For Quantitative, this formula takes the average of quantitative scores in an assessment instance. The scores are contributed by scores corresponding to the factors that a comprise a group factor and have factor contribution of either Quantitative or Both.

Product

For Qualitative, this formula multiplies qualitative scores in an assessment instance. The scores are contributed by scores corresponding to the factors that a comprise a group factor and have factor contribution of either Qualitative or Both.

For Quantitative, this formula multiplies quantitative scores in an assessment instance. The scores are contributed by scores corresponding to the factors that a comprise a group factor and have factor contribution of either Quantitative or Both.

Weighted average

For Qualitative, this formula divides the sum of qualitative scores in an assessment instance by the sum of weights. The scores are contributed by scores corresponding to the factors that a comprise a group factor and have factor contribution of either Qualitative or Both.

### Create an automated factor

Create automated factors to automatically fetch data from other data sources such as tables or database views.

**Before you begin**

You must have the Governance, Risk, and Compliance Enterprise license.

Role required: sn_risk.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

Automated factors help automate the risk assessment process. They do not to rely on manual inputs, and they thus reduce subjectivity. All the responses to automated factors are automatically calculated during the assessment.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Automated Factors**.
2. Click **New**.
3. On the form, fill in the fields.

#### Automated Query Factor form

| Field | Description |
|---|---|
| Name | Name of the factor such as `Regulatory Impact`. |
| Factor contribution | Type of factor contribution. Choices are the following:<br>◦ **Qualitative**: Provides a numerical score and then converts the score into a rating.<br>◦ **Quantitative**: Provides the losses that can be incurred in monetary terms. The losses contribute to the annual loss expectancy (ALE).<br>◦ **Both**: Assessment type is both qualitative and quantitative. |
| Display order | Order of questions in the assessment form. This field enables you to set a specific sequence in which the questions must appear. |
| Response type | Options for users to respond to the factors. Choices are the following:<br>◦ **Number**: The factor response after automatic calculation will be a number.<br>◦ **Currency**: The factor response after automatic calculation will be in currency.<br>◦ **Percentage**: The factor response after automatic calculation will be a percentage. |
| Assessment context | Context where the assessment must be performed. Choices are the following:<br>◦ **Risk**: Select this option to perform the assessment for an entity and for an associated risk.<br>◦ **Object**: Select this option to perform an assessment on any ServiceNow record. For example, users can perform Exception Risk Assessment or Change Risk Assessment directly on an object. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| State | State of the factor. This field is automatically set to **Draft**. |
| Qualitative weighting (%) | Score contribution or qualitative weight that is given to the factor. This value determines the actual contribution of this factor to the final score. This field appears only when **Qualitative** is selected from the **Factor contribution** field. |
| Transform qualitative score | Option to transform the overall group qualitative score based on an interval scale.<br><br>For example, assume the **User response** field is set to **Percentage**. As the admin, you can transform the percentage value into a qualitative score, such that 0% to 30% is low, 30% to 60% is medium, and 60% and higher is high. In this case, the ratings 1, 2, and 3 can be assigned to low, medium, and high.<br><br>This field appears only when **Qualitative** is selected from the**Factor contribution** field. |
| Collect supporting data | Option for collecting supporting data. If this option is selected, the Supporting Data section appears. |
| Description | Brief description about the purpose of the factor and where to use the factor. This description is for the administrator to understand the factor. |
| Data Source | |
| Source | Table or view that is used as the source of the factor. |
| Filter Criteria | |
| Filter by entity | Option for filtering the source by the risk assessment instance entity. |
| Entity-mapping field | Field that refers to the Entity table. This field appears only when the **Filter by entity** option is selected. |
| Filter by risk | Option for filtering the source by the risk of the risk assessment instance. |
| Risk mapping field | Field that refers to the Risk table. This field appears only when the **Filter by risk** option is selected. |
| Filter by control | Option for filtering the source by the risk assessment instance control. This option applies only to the individual assessment of controls in the control assessment. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Control mapping field | Field that refers to the Control table. This field appears only when the **Filter by control** option is selected. |
| Filter by object | Option for filtering the source by the object of the risk assessment instance. This field appears only when you are performing the risk assessment on an object. |
| Object mapping field | Field that refers to an object in the assessment instance. This field appears only when **Object** is selected from the **Assessment context** field, and when the **Filter by object** option is selected. |
| Aggregation. | |
| Aggregation type | Formula for aggregating the records that are selected from the table in the **Source** field. Choices are the following:<br>◦ **Sum**: Sum of the aggregation column.<br>◦ **Average**: Average value of the aggregation column.<br>◦ **Maximum**: Maximum value of the aggregation column.<br>◦ **Minimum**: Minimum value the aggregation column.<br>◦ **Count**: Count of number of records of the aggregation column.<br>◦ **Count distinct**: Number of unique records of the aggregation column. |
| Aggregation column | Column that is used for aggregation based on the table selected in the **Source** field. |
| Schedule | |
| Frequency | Frequency of when the factor is run. |
| Day of the week | Day of the week when the factor is run. This field appears only when **Weekly** is selected from the **Frequency** field. |
| Day of month | Day of the month when the factor is run. This field appears only when **Monthly** is selected from the **Frequency** field. |
| Month | Month when the factor is run. This field appears only when the **Frequency** field has the values **Quarterly**, **Semi-annually**, or **Annually**. |
| Next run date | Date when the factor runs again. This field is automatically set based on the selections made on the form. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Click the Supporting Data section.
5. For the data that you want to collect, move the corresponding fields from the Available list to the Selected list.
6. Click **Submit**.
7. Open the factor that you created.
8. Click **Publish**.

### Result
The factor is published and is ready for use in a Risk Assessment Methodology.

Related topics

Create a scripted automated factor

## Create a scripted automated factor

Create scripted automated factors that use a script to fetch data from ServiceNow® records or from external sources. During risk assessment, scripted automated factors automatically calculate and provide the responses for factors.

### Before you begin
Role required: sn_grc.developer and sn_risk.admin

### Procedure
1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Automated Scripted Factors**.
2. Click **New**.
3. On the form, fill in the fields.

**Automated Scripted Factor form**

| Field | Description |
|---|---|
| Name | Name of the factor such as `Regulatory Impact`. |
| Factor contribution | Type of factor contribution. Choices are the following:<br>◦ **Qualitative**: Provides a numerical score and then converts the score into a rating.<br>◦ **Quantitative**: Provides the losses that can be incurred from a risk in monetary terms. The losses contribute to the annual loss expectancy (ALE).<br>◦ **Both**: Assessment type is both qualitative and quantitative. |
| Display order | Order of questions in the assessment form. This field enables you to set a specific sequence in which the questions must appear. |
| Response type | Options for users to respond to the factors. Choices are the following: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ **Number**: The factor response after automatic calculation will be a number.<br>◦ **Currency**: The factor response after automatic calculation will be in currency.<br>◦ **Percentage**: The factor response after automatic calculation will be in percentage. |
| Transform qualitative score | Option to transform the overall group qualitative score based on an interval scale.<br><br>For example, assume the **User response** field is set to **Percentage**. As the admin, you can transform the percentage value into a qualitative score, such that 0% to 30% is low, 30% to 60% is medium, and 60% and higher is high. In this case, the ratings 1, 2, and 3 can be assigned to low, medium, and high.<br><br>This field appears only when **Qualitative** is selected from the**Factor contribution** field. |
| State | State of the factor. This field is automatically set to **Draft**. |
| Qualitative weighting (%) | Score contribution or qualitative weight that is given to a factor. This value determines the actual contribution of this factor to the final score. This field appears only when **Qualitative** is selected from the **Factor contribution** field. |
| Assessment context | Context for which the assessment must be performed. Choices are the following:<br>◦ **Risk**: Select this option to perform the assessment for an entity and its associated risk.<br>◦ **Object**: Select this option to perform an assessment on any ServiceNow record. For example, users can perform Exception Risk Assessment or Change Risk Assessment directly on an object. |
| Description | Brief description about the purpose of the factor and where to use the factor. This description is for the administrator to understand the factor. |
| Script | |
| Variables | Predefined variables to be used in the **Script** field. |
| Script | Custom script. |
| Schedule | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Frequency | Frequency of when factor is run. |
| Day of the week | Day of the week when the factor is run. This field appears only when the **Frequency** field has **Weekly**. |
| Day of month | Day of the month when the factor is run. This field appears only when the **Frequency** field has **Monthly**. |
| Month | Month when the factor is run. This field appears only when the **Frequency** field has **Quarterly**, or **Semi-annually**, **Annually**. |
| Next run date | Date when the factor is run again. This field is automatically set based on the selections made on the form. |

4. Click **Submit**.
5. Open the factor that you created.
6. Click **Publish**.

### Result
The factor is published and is ready for use in a Risk Assessment Methodology.

Related topics

Create an automated factor

## Copy a factor

Create a copy of a published factor to make minor modifications and then reuse the factor.

### Before you begin
Role required: sn_risk.admin

### Procedure
1. Navigate to **All** > **Advanced Risk Assessment** > **Administration**
2. Open the factor you want to copy.
3. Click **Copy**.

### Result
A copy of the factor is created.

## Configure a risk assessment methodology

Configure a risk assessment methodology (RAM) in the Advanced Risk application so that you can assess the risks or objects in your organization.

### Before you begin
Role required: sn_risk_advanced.ara_admin

### About this task
A RAM is a configuration or record in the new risk assessment engine in the Advanced Risk application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can use a RAM to assess either the risks or objects in your organization. For example, you can configure a RAM to specify the types of risk assessments and the entities on which a risk assessment is performed. By using a RAM, your organization can have different methodologies for assessing risks.

After you move a RAM to the **Retired** state, you can also move it back to the **Draft** state if you want to make some changes later. You can only move a RAM to the **Draft** state if it doesn't have any assessments in the **Monitor** state or the **Closed** state. When you move a RAM back to the **Draft**, the on-going assessments and the associated scopes are deleted.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Risk Assessment Methodologies**.
2. Select **New**.
3. On the form, fill in the fields.

   For a description of the field values on the risk assessment methodology form, see Risk Assessment Methodology form.
4. Right-click and save the form.
5. To configure the various assessments, select one of the following options.

| Choice | Related link |
|---|---|
| Configure inherent assessment | See Configure an inherent assessment. |
| Configure control effectiveness | See Configure a control effectiveness assessment |
| Configure residual assessment | See Configure a residual assessment |
| Configure target assessment | See Configure a target assessment |

6. Select **Publish**.

> **Note:** After a new assessment is created on the same risk and the assessment is in the **Monitor** state, the other assessments automatically move to the **Completed** state. When an assessment instance is in the **Monitor** state, you can't move the RAM back to the **Draft** state. A RAM can only be moved back to the **Draft** state if there are no assessment instances.

#### Risk Assessment Methodology form

Use the Risk Assessment Methodology form in the Advanced Risk application to specify the types of risk assessments and the entities on which the risk assessment is performed.

See the following table for a description of the field values.

**Risk Assessment Methodology form**

| Field | Description |
|---|---|
| Name | Name of the risk assessment methodology (RAM). For example, Organizational risk assessment. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk Assessment Methodology form (continued)**

| Field | Description |
|---|---|
| Domain area | Domain area of the RAM. This field is automatically set to **IRM**. |
| State | State of the RAM. This field is automatically set to **Draft**. |
| Assessment Context | |
| Assess | Assessment context that you can select:<br>• **Risk**: Performs the assessment for an entity and the risk statement that is related to it.<br>• **Object**: Performs an assessment on any ServiceNow record. For example, users can perform an Exception Risk Assessment or a Change Risk Assessment directly on those respective tables. |
| Applicable entity classes | All entity classes that the RAM applies to, such as the business services, assets, or business applications. This field appears only when **Risk** is selected from **Assess**. |
| Applicable Record Types | Tables on which you want to perform the assessment. You can select multiple tables and associate them to the RAM. This field appears only when **Object** is selected from **Assess**.<br>**Note:** You can add multiple objects or tables to a published RAM, but can't remove them after the RAM is published. |
| Workflows | |
| Inherent risk | Option for assessing an inherent risk. |
| Control effectiveness | Option for assessing the control effectiveness. |
| Enable risk response | Option to enable the **Risk Response** tab on the risk assessment. This option appears only when **Risk** is selected from **Assess**. |
| Residual risk | Option for assessing a residual risk. |
| Target risk | Option for assessing a target risk. |
| Rollup Configurations | |
| This section appears only when **Risk** is selected from **Assess**. | |
| Calculate ALE based on | Formula that you can select for calculating the annual loss expectancy (ALE): |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk Assessment Methodology form (continued)**

| Field | Description |
|---|---|
| | • **Sum**<br>• **Average**<br>• **Maximum**<br>• **Minimum** |
| Calculate score based on | Formula that you can select for calculating the score:<br>• **Average**<br>• **Maximum**<br>• **Minimum** |
| Risk Response Configurations | |
| This section appears only when **Risk** is selected from **Assess**. | |
| Allow single risk response | Option to make the risk response selection a single select in the risk assessment form. For example, the options could be "Accept," "Avoid," "Mitigate," or "Transfer." With a single select, assessors can choose only one of these options to indicate the risk response strategy.<br>**Note:** This option can only be enabled when there are no ongoing assessments. |
| Risk response is required | Option to make a risk response as required:<br>• **None**: No risk response is required.<br>• **Always**: Mandate a risk response always.<br>• **On specific conditions**: Mandate a risk response based on specific conditions using the condition builder.<br>• **On specific conditions defined using script**: Mandate a risk response under specific conditions using a predefined script or set of instructions. |
| Business Rules and Validations | |
| Final comment is required | Option to make the final comments as required. Final comments provide better transparency and enable risk owners to communicate the action plan if there's a breach of appetite or tolerance. The options are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk Assessment Methodology form (continued)**

| Field | Description |
|---|---|
| | • **None**: No final comment is required.<br>• **Always**: Mandate final comments always.<br>• **On breach of appetite**: Mandate final comments on the breach of appetite.<br>• **On breach of tolerance**: Mandate final comments on the breach of tolerance.<br><br>This field appears only when **Risk** is selected from **Assess**. |
| Automatically create issue | Option to create issues automatically. This field appears only when **Risk** is selected from **Assess**.<br>• **None**: Enables you not to create issues automatically.<br>• **On breach of appetite**: Creates issues automatically on the breach of appetite.<br>• **On breach of tolerance**: Creates issues automatically on the breach of tolerance.<br><br>**Note:** The issues are created only after the risk assessment is approved and moved to the published state. |
| Residual score is lower than inherent | Option to validate that the qualitative residual score is lower than the inherent score.<br><br>**Note:** This option appears only when the residual risk assessment is enabled. |
| Reference Information | |
| This section appears only when **Risk** is selected from **Assess**. Enabling these options shows the reference information in the risk assessment instance. | |
| Show related risk events | Option for showing the related risk events on the risk assessment. |
| Show related risk indicators | Option for showing the related risk indicators on the risk assessment. |
| Show open issues | Option for showing the open issues on the risk assessment. |
| Show previous assessment | Option for showing the previous assessment on the risk assessment. This option helps the risk assessor to refer to the previous assessment and analyze the details of that assessment before taking another assessment. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk Assessment Methodology form (continued)**

| Field | Description |
|---|---|
| Other Configurations | |
| Advanced reminder (days) | Based on the due date of the risk assessment, this field is the number of days before a notification is sent to the assessor. For example, if you enter 3 in this field, then the assessor gets a reminder notification three days before the due date. |
| Overdue reminder (days) | Based on the due date of the risk assessment, this field is the number of days after this date that reminder emails are sent. For example, assume you enter 5 in this field. Then for five days after the due date is over, the assessor keeps receiving reminder emails that the due date is over. On the sixth day, an email notification is sent to the assessor and to the assessor's manager. |
| Risk identification | Method to identify risks in the risk assessment scope:<br>• **None**<br>• **From Library**: Identifies risks from the library on the risk assessment.<br>• **Ad-hoc**: Identifies a risk that is not in the library.<br>• **From Library and Ad-hoc**: Creates risks as well as adds risks from the library. |
| Group factor comments | Option to enable group factor comments in the risk assessment form. |
| Copy previous responses | Option to copy the factor responses and comments whenever a reassessment is performed. |
| Allow override of results | Option to override the computed scores and the ALE during risk assessment. |
| Configure section terminology | Option to configure section labels for inherent, control, residual, and target assessments. After you select this option, you can configure the title, score label, and annual loss expectancy label for each assessment type.<br>**Note:** Section label renaming applies only to the advanced risk assessment interface while leaving the terminology used in reports, dashboards, heatmaps, and other areas unchanged. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk Assessment Methodology form (continued)**

| Field | Description |
|---|---|
| Update assessment results to source record | Option to copy the assessment results to the source record on which the assessment is performed. You can define the assessment result mapping for the applicable record types in the individual assessment types. This field appears only when **Object** is selected from **Assess**. |
| Schedule | |
| This section appears only when **Object** is selected from **Assess**. | |
| Reassessment frequency | Option of how often the reassessment is performed:<br>• **None**<br>• **Weekly**<br>• **Monthly**<br>• **Quarterly**<br>• **Semi-annually**<br>• **Annually** |
| Days to overdue | Based on the due date of the risk assessment, this field is the number of days after which an assessment is considered overdue. |

### Copy a risk assessment methodology

Modify your risk assessment methodology (RAM) and factors by creating a copy of the record. The option to copy allows the system to create a true copy of the underlying record including all the related lists. This action saves the time of risk administrators as they do not have to create the records from the beginning each time.

#### Before you begin

Role required: sn_risk.admin

#### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Risk Assessment Methodologies**
2. Open the RAM you want to copy.
3. Click **Copy**.

### Retire a risk assessment methodology

Retire a risk assessment methodology (RAM) that is no longer used. Retiring unused RAMs makes it easier to manage the active RAMs for the risk administrator.

#### Before you begin

Role required: sn_risk.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

When you retire a risk assessment methodology, it is important to note that you cannot make a retired RAM active again. You must also note that:

- all the factors associated with this methodology retire.
- the risk assessment scope retires.
- all open associated assessments retire.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Risk Assessment Methodologies**.
2. Select and open the risk assessment methodology that you want to retire.
3. Click **Retire**.
   The state changes to **Retired**.

## Configure an inherent assessment

Configure and publish an inherent assessment in the Advanced Risk application to assess the inherent risks in your organization.

### Before you begin

Role required: sn_risk.admin

### About this task

Configure the criteria for an inherent risk assessment by adding the factors, scoring logic, and rating criteria to the Inherent Assessment form. Each risk assessment methodology (RAM) has its own inherent assessment criteria. For example, you can assess the inherent risk for such factors as the financial impact, regulatory impact, and client impact. To get the inherent assessment score, the impact of these factors is multiplied by the likelihood that a risk would occur.

### Procedure

1. Navigate to the RAM form that has the inherent risk as an assessment type.
2. In the Assessment Types related list, select **Inherent Assessment**.
3. On the form, fill in the fields.

   For a description of the field values on the inherent assessment form, see Inherent Assessment form.

4. To add factors, select the Factors related list.
   This related list is available only when **Factor responses** is selected from the **Calculate based on** field.
5. Select **Edit** and add the factors.
6. Select **Save**.
7. Select the Qualitative Rating Criteria related list and select **New**.
8. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Qualitative Rating Criteria form**

| Field | Description |
|---|---|
| Lower rating interval | Range for qualitative risk ratings. For example, for a range of 0–10, you can enter 0 as the lower range. For a range of 11– 20, the value can be 11 as the lower range. |
| Rating | Severity of the risk. You can enter ratings such as high, medium, or low. For example, assume that the lower rating interval for the Low rating is 0, and that the lower rating interval for the Medium rating is 11. If the risk score is 15, then the rating criterion is Medium because 15 is in the range of 11-20. |
| Overridden score | Score that is used when the assessor overrides the risk rating. |
| Risk color style | Color code style for the background color on the risk rating value and for the text color on the risk assessment instance. For example, for a high risk, you can select the Red color style with the background color as red and the text as black. |
| Risk appetite scale | Risk appetite scale for the risk rating criteria. The appetite scales must be mapped to the qualitative risk rating criteria in the risk assessment methodology. You can compute the qualitative appetite status that is based on the latest assessment or aggregated rating to provide the qualitative appetite status. For example, you can select a risk appetite scale of **Hungry** for the risk rating of **Very High**. This field appears only when the risk appetite feature is configured in the advanced risk assessment properties.<br><br>**Important:** In a qualitative risk assessment, map the risk appetite scale to the risk rating criteria for the final assessment type. For example, if you have both residual and inherent assessments, map the risk appetite scale to the risk rating criteria in the residual assessment. |

**Note:** Don't enter negative values in the Qualitative Rating Criteria form.

9. Optional: If you select the **Enable heatmap** option, then do the following actions:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select the Heatmap Colors related list.

b. In the Risk color style column, specify the risk color style.

10. To define the assessment result mapping for the applicable record types, do the following actions:

    These steps apply when conducting the inherent assessment on an object.

    a. Select the Assessment Result Mapping related list.
    The Assessment Result Mapping related list appears only when the **Update assessment results to source record** option is selected in the RAM.

    b. Select the record type.

    c. On the form, fill in the fields.

**Applicable Record Type form**

| Field | Description |
|---|---|
| Risk assessment methodology | Name of the RAM. This field is automatically set based on the selected RAM. |
| Record Type | Name of the applicable record type. This field is automatically set based on the selected record type. |
| Inherent risk rating | Column where the inherent risk rating value is stored in the source record. After the assessment, the inherent risk rating result is copied to the column that is selected in this field. This field appears only when the **Assessment contribution** field has **Qualitative** or **Both**. |
| Inherent ALE | Column where the inherent annual loss expectancy (ALE) value is stored in the source record. After the assessment, the inherent ALE result is copied to the column that is selected in this field. This field appears only when the **Assessment contribution** field is set to is **Quantitative** or **Both**. |

**Note:** If the same record type is used in another risk assessment methodology, the source record will update based on the field defined in the RAM of the latest advanced risk assessment.

    d. Select **Update**.

11. Select **Submit**.

12. Select **Publish**.

**Result**
The assessment type is published.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Inherent Assessment form

Use the Inherent Assessment form in the Advanced Risk application to assess the inherent risks in your organization.

See the following table for a description of the field values.

#### Inherent Assessment form

| Field | Description |
|---|---|
| Risk assessment methodology | Selected RAM. This field is automatically set based on your RAM. |
| State | State of the RAM. This field is automatically set to **Draft**. |
| Calculate based on | Option for calculating the assessment score that is based on factor responses. |
| Assessment contribution | Type of factor contribution:<br>• **Qualitative**: Provides a numerical score and then converts the score into a rating. Selecting this option ensures that only qualitative factors are available for adding.<br>• **Quantitative**: Provides the losses that can be incurred in monetary terms. The losses contribute to the annual loss expectancy (ALE). Selecting this option ensures that only quantitative factors are available for adding.<br>• **Both**: Provides both the qualitative and quantitative assessment type. |
| Enable heatmap | Option to enable the heatmap report on the Advanced Risk dashboard.<br>**Note:** You can select this option only if a minimum of two factors are added to the assessment type. Selecting this option makes the Heatmap Configuration section and the Heatmap Colors related list appear on the form. |
| Qualitative Score | |
| This section appears only when **Qualitative** is selected from the **Assessment contribution** field. | |
| Qualitative scoring logic | Formula that you can use to calculate the scoring logic: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Inherent Assessment form (continued)**

| Field | Description |
|---|---|
| | • **Sum**: Sum of the factor responses.<br>• **Minimum**: Minimum value of the factor responses.<br>• **Maximum**: Maximum value of the factor responses.<br>• **Average**: Average value of the factor responses.<br>• **Product**: Value that is derived by multiplying the factor responses.<br>• **Weighted average**: Average value of the weighting of factors. This value is then classified as low, medium, or high.<br>• **Script**: User-defined formula to calculate the score. This option is available only to users with the sn_grc.developer role. |
| Quantitative Score | |
| This section appears only when **Quantitative** is selected from the **Assessment contribution** field. | |
| Quantitative scoring logic | Formula that you can use to calculate the scoring logic:<br>• **Sum**: Sum of the factor responses.<br>• **Minimum**: Minimum value of the factor responses.<br>• **Maximum**: Maximum value of the factor responses.<br>• **Average**: Average value of the factor responses.<br>• **Product**: Value that is derived by multiplying the factor responses.<br>• **Script**: User-defined formula to calculate the score. This option is available only to users with the sn_grc.developer role. |
| Section Labels | |
| This section appears only when **Configure section terminology** is selected in the RAM form.<br>**Note:** Section label renaming applies only to the advanced risk assessment interface while leaving the terminology used in reports, dashboards, heatmaps, and other areas unchanged. | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Inherent Assessment form (continued)**

| Field | Description |
|---|---|
| Title | Option to rename the section title of the assessment type. For example, if you rename Inherent assessment as Gross assessment, the new title will be displayed in all sections where the Inherent assessment was previously referred. |
| Score label | Option to rename the qualitative score label in the Scoring section of the assessment form. For example, if you rename Inherent risk as Gross risk, the new score label will be displayed in the scoring section where Inherent risk was previously referred. |
| Annual loss expectancy label | Option to rename the quantitative score label in the Scoring section of the assessment form. For example, if you rename Inherent ALE as Gross ALE, the new score label will be displayed in the scoring section where Inherent ALE was previously referred. |
| Heatmap Configuration | |
| This section appears only when the **Enable heatmap** option is selected. | |
| Factor for X-axis | Factor that appears on the X-axis of the heatmap.<br>**Note:** Only qualitative factors of the type **Choice** or factors with the transformation criteria can be selected. For more information, see Transformation criteria. |
| Factor for Y-axis | Factor that appears on the Y-axis of the heatmap.<br>**Note:** Only qualitative factors of the type **Choice** or with the transformation criteria can be selected. For more information, see Transformation criteria. |

### Configure a control effectiveness assessment

Configure and publish a control effectiveness assessment to assess the effectiveness of controls in mitigating risks.

#### Before you begin

Role required: sn_risk.admin

#### About this task

Configure the control assessment criteria with details such as factors, the scoring logic, and the rating criteria. You can also specify if you would like to assess the complete control environment or if you would like to assess controls individually. These details are the aspects

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

on which the risk assessment is performed. You can also enable the options to add existing controls or new controls during an assessment. This exercise ensures that each risk assessment methodology (RAM) has its own control assessment criteria.

### Procedure

1. Navigate to the RAM form that has inherent risk as an assessment type.
2. Under the Assessment Types related list, select **Control Assessment**.
3. On the form, fill in the fields.

   For a description of the field values on the control assessment form, see Control Assessment form.

4. Select the Factors section and select **Edit**.
   The Factors related list appears only when **Control environment assessment** is selected from the **Calculate based on** field.
5. Add the necessary factors from the Collection list to the Factors list, and select **Save**.
6. Select the Qualitative Rating Criteria related list and select **New**.
7. On the form, fill in the fields.

**Qualitative Rating Criteria form**

| Field | Description |
|---|---|
| Lower rating interval | Range for qualitative risk ratings. For example, for a range of 0–10, you can enter 0 as the lower range. And for a range of 11– 20, the value can be 11 as the lower range. |
| Risk rating | Severity of the risk. You can enter ratings such as high, medium, or low. For example, assume that the lower rating interval for the Low rating is 0, and that the lower rating interval for the Medium rating is 11. If the risk score is 15, then the rating criterion is Medium because 15 is in the range of 11–20. |
| Overridden score | Score that the risk assessor can use to override the computed score. |
| Risk color style | Color code style for the background color on the risk rating value and for the text color on the risk assessment instance. For example, for a high risk, you can select the Red color style with the background color as red and the text as black. |

**Note:** Don't enter negative values in the Qualitative Rating Criteria form.

8. To define the assessment result mapping for the applicable record types, do the following actions:

   These steps apply when conducting the control assessment on an object.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select the Assessment Result Mapping related list.
The Assessment Result Mapping related list appears only when the **Update assessment results to source record** option is selected in the RAM.

b. Select the record type.

c. On the form, fill in the fields.

**Applicable Record Type form**

| Field | Description |
|---|---|
| Risk assessment methodology | Name of the RAM. This field is automatically set based on the selected RAM. |
| Record Type | Name of the applicable record type. This field is automatically set based on the selected record type. |
| Control effectiveness | Column where the control effectiveness rating value is stored in the source record. After the assessment, the control effectiveness result is copied to the column selected in this field. |

**Note:** If the same record type is used in another risk assessment methodology, the source record will update based on the field defined in the RAM of the latest advanced risk assessment.

d. Select **Update**.

9. Select **Submit**.
10. Select **Publish**.

**Result**
The control assessment type is published.

**Control Assessment form**

Use the Control Assessment form in the Advanced Risk application to assess the effectiveness of controls in mitigating risks.

See the following table for a description of the field values.

**Control Assessment form**

| Field | Description |
|---|---|
| Risk assessment methodology | Name of the risk assessment methodology used for control assessment. This field is automatically set based on your RAM. |
| State | State of the RAM. This field is automatically set to **Draft**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Control Assessment form (continued)**

| Field | Description |
|---|---|
| Assessment contribution | Type of factor contribution. This field is automatically set to **Qualitative contribution**. |
| Calculate based on | Option to assess the types of control. Choices are the following:<br>• **Control environment assessment**: Select this option if you don't want to assess individual controls, but instead want to assess the overall effectiveness of the control environment.<br>• **Individual assessment of controls**: Select this option if you want to perform assessment for individual controls. For example, you can select the risk of employees accepting bribes and then assess each existing control to mitigate the risk of bribery. This option is available only when the Policy and Compliance Management (com.sn_compliance) plugin is activated. |
| Control identification | Option to decide how to identify the controls in the risk assessment instance. The choices are the following:<br>• **None**<br>• **From Library**: Use this option when you want to identify controls from the library on the risk assessment instance.<br>• **Ad-hoc**: Use this option when you want to identify new controls on the risk assessment instance.<br>• **From Library and Ad-hoc**: Use this option when you want to identify controls from the library as well as identify new controls.<br><br>This field appears only when the **Calculate based on** field has the value **Individual assessment of controls**. |
| Factor for overall effectiveness | Manual, automated, or group factors to assess controls. This field appears only when the option **Individual assessment of controls** is selected from the **Calculate based on** field. Only qualitative factors or factors with the option to transform the qualitative score will be displayed in this field. |
| Qualitative scoring logic | Formula for calculating the scoring logic. Choices are the following: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Control Assessment form (continued)**

| Field | Description |
|---|---|
| | • **Sum**: Sum of the factor responses.<br>• **Minimum**: Minimum value of the factor responses.<br>• **Maximum**: Maximum value of the factor responses.<br>• **Average**: Average value of the factor responses.<br>• **Product**: Value derived by multiplying the factor responses.<br>• **Weighted average**: Average value of the weighting of factors. This value is then classified as low, medium, or high. When this option is selected, the control weight is fetched from the control form.<br>• **Script**: User-defined formula to calculate the score. This option is available only to users with the sn_grc.developer role. |
| Qualitative script variables | Format of the script and the variables used in the script. This field is available only when **Script** is selected from the **Qualitative scoring logic** field. |
| Qualitative script | User-defined script to compute the scoring logic. This field enables you to have more control over the score computation. |
| Section Labels | |
| This section appears only when **Configure section terminology** is selected in the RAM form.<br>**Note:** Section label renaming applies only to the advanced risk assessment interface while leaving the terminology used in reports, dashboards, heatmaps, and other areas unchanged. | |
| Title | Option to rename the section title of the assessment type. For example, if you rename Control assessment as Preventive assessment, the new title will be displayed in all sections where the Control assessment was previously referred. |
| Score label | Option to rename the qualitative score label in the Scoring section of the assessment form. For example, if you rename Control risk as Preventive risk, the new score label will be displayed in the scoring section where Control risk was previously referred. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Configure a residual assessment

Configure and publish a residual assessment in the Advanced Risk application to assess the residual risks in your organization.

## Before you begin

Role required: sn_risk.admin

## About this task

Use a residual assessment to identify and assess the risks that exist after any controls are implemented. If no controls are identified, then the residual risk is the same as an inherent risk. If the factors for an inherent assessment are used a residual assessment, then you can copy the assessment contribution, qualitative scoring logic, factors, and qualitative rating criteria from the inherent assessment. You can also choose how you want to derive the score of the residual assessment.

## Procedure

1. Navigate to the risk assessment methodology (RAM) form that has the residual risk as an assessment type.
2. In the Assessment Types related list, select **Residual Assessment**.
3. On the form, fill in the fields.

   For a description of the field values on the residual assessment form, see Residual Assessment form.
4. Optional: If you selected **Factor responses** in the **Calculate based on** field, then select the Factors related list so that you can add factors to the residual assessment.
5. Select **Edit**, add the necessary factors, and then select **Save**.
6. Optional: If the **Calculate based on** field has **Inherent risk and control effectiveness** and if the **Qualitative scoring logic** field has **Lookup matrix between inherent assessment and control effectiveness**, then do the following actions:
   a. Select the Matrix related list.
   b. In the respective columns, enter the score, risk rating, risk color style, and overridden score.
7. Select the Qualitative Rating Criteria related list and select **New**.
8. On the form, fill in the fields.

### Qualitative Rating Criteria form

| Field | Description |
|---|---|
| Lower rating interval | Range for the qualitative risk ratings. For example, for a range of 0–10, you can enter 0 as the lower range. For a range of 11– 20, the value can be 11 as the lower range. |
| Risk rating | Severity of the risk. You can enter ratings such as high, medium, or low. For example, assume that the lower rating interval for the Low rating is 0, and that the lower rating interval for the Medium rating is 11. If the risk score is 15, then the rating criterion is |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | Medium because 15 is in the range of 11–20. |
| Overridden score | Score that the risk assessor can use to override the computed score. |
| Risk color style | Color code style for the background color on the risk rating value and for the text color on the risk assessment instance. For example, for a high risk, you can select the Red color style with the background color as red and the text as black. |
| Risk appetite scale | Risk appetite scale for the risk rating criteria. Appetite scales must be mapped to the qualitative risk rating criteria in the risk assessment methodology. Compute the qualitative appetite status that is based on the latest assessment or aggregated rating to provide the qualitative appetite status. For example, you can select a risk appetite scale of **Hungry** for the risk rating of **Very High**. This field appears only when the risk appetite feature is configured in the advanced risk assessment properties.<br><br>**Important:** In a qualitative risk assessment, map the risk appetite scale to the risk rating criteria for the final assessment type. For example, if you have both residual and inherent assessments, map the risk appetite scale to the risk rating criteria in the residual assessment. |

**Note:** Don't enter negative values in the Qualitative Rating Criteria form.

9. Select the Heatmap Colors related list.
   This related list appears only when all of the following are true:
   - The **Enable heatmap** option is selected.
   - The **Calculate based on** field has **Factor responses**.
   - The residual assessment is based on a matrix between the inherent assessment and control effectiveness.
10. In the Risk color style column, select the background color and text color combination.
11. To define the assessment result mapping for the applicable record types, do the following actions:

    These steps apply when conducting the residual assessment on an object.

    a. Select the Assessment Result Mapping related list.
       The Assessment Result Mapping related list appears only when the **Update assessment results to source record** option is selected in the RAM.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**b.** Select the record type.

**c.** On the form, fill in the fields.

**Applicable Record Type form**

| Field | Description |
|---|---|
| Risk assessment methodology | Name of the RAM. This field is automatically set based on the selected RAM. |
| Record Type | Name of the applicable record type. This field is automatically set based on the selected record type. |
| Residual risk rating | Column where the residual risk rating value is stored in the source record. After the assessment, the residual risk rating result is copied to the column that is selected in this field. This field appears only when the **Assessment contribution** field has **Qualitative** or **Both**. |
| Residual ALE | Column where the residual annual loss expectancy (ALE) value is stored in the source record. After the assessment, the residual ALE result is copied to the column that is selected in this field. This field appears only when the **Assessment contribution** field is set to is **Quantitative** or **Both**. |

**Note:** If the same record type is used in another risk assessment methodology, the source record will update based on the field defined in the RAM of the latest advanced risk assessment.

**d.** Select **Update**.

**12.** Select **Submit** and then select **Publish**.

### Result

The assessment type is published.

#### Residual Assessment form

Use the Residual Assessment form in the Advanced Risk application to assess the residual risks in your organization.

See the following table for a description of the field values.

**Residual Assessment form**

| Field | Description |
|---|---|
| Risk assessment methodology | Name of the RAM. This field is automatically set based on the selected RAM. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Residual Assessment form (continued)**

| Field | Description |
|---|---|
| Calculate based on | Options for calculating the assessment score:<br>• **Inherent risk and control effectiveness**: Makes the assessment qualitative. The comparison between inherent and control effectiveness is always qualitative.<br>• **Factor responses**: Bases the residual factors' calculation on responses to manual factors. |
| Assessment contribution | Type of factor contribution:<br>• **Quantitative**<br>• **Qualitative**<br>• **Both**<br><br>If **Inherent risk and control effectiveness** is selected in the **Calculate based on** field, then this field is automatically set to **Qualitative**. The field can't be modified. |
| Factors same as inherent | Option to automatically copy the assessment contribution, qualitative scoring logic, factors, and qualitative rating criteria from the inherent assessment.<br><br>**Note:** This option appears only when the **Calculate based on field** field has the **Factor responses** value. |
| Enable heatmap | Option to enable you to view the heatmap report on the Advanced Risk dashboard.<br><br>**Note:** This option can be selected only if a minimum of two factors are added to the assessment type. |
| Qualitative score | |
| Qualitative scoring logic | Scoring logic to be used. The options for this field change based on the option that is selected in the **Calculate based on** field.<br><br>When the **Calculate based on** field has **Inherent risk and control effectiveness**, the options are as follows:<br>• **Lookup matrix between inherent assessment and control effectiveness**: Generates a matrix between the inherent assessment and control effectiveness assessment. It performs a Cartesian |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Residual Assessment form (continued)**

| Field | Description |
|---|---|
| | product to generate scores. You can view the matrix in the Matrix related list. For example, if the inherent risk is high and the control effectiveness is low, then the residual risk is also high.<br>• **Inherent score-control effectiveness score**: Provides the difference between the inherent score and the control effectiveness score.<br>• **Inherent score/control effectiveness score**: Provides the value that is derived by dividing the inherent score by the control effectiveness score.<br>• **Script**: Use a custom script to calculate the qualitative score. The Script option enables you to create a customized calculation method that aligns with your organization's unique requirements and risk assessment approach.<br>**Note:** You can write or modify scripts only for assessment types that aren't published.<br>When the **Calculate based on** field has **Factor responses**, the options are as follows:<br>• **Sum**: Sum of the factor responses.<br>• **Minimum**: Minimum value of the factor responses.<br>• **Maximum**: Maximum value of the factor responses.<br>• **Average**: Average value of the factor responses.<br>• **Product**: Value derived by multiplying the factor responses.<br>• **Weighted average**: Average value of the weighting of factors. This value is then classified as low, medium, or high.<br>• **Script**: User-defined formula to calculate the score. This option is available only to users with the sn_grc.developer role. |
| Quantitative score | |
| This section appears only when the value **Quantitative** is selected from the **Factor contribution** field. | |
| Quantitative scoring logic | Scoring logic to be used: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Residual Assessment form (continued)**

| Field | Description |
|---|---|
| | • **Sum**: Sum of the factor responses.<br>• **Minimum**: Minimum value of the factor responses.<br>• **Maximum**: Maximum value of the factor responses.<br>• **Average**: Average value of the factor responses.<br>• **Product**: Value that is derived by multiplying the factor responses.<br>• **Script**: User-defined formula to calculate the score. This option is available only to users with the sn_grc.developer role. |
| Section Labels | |
| This section appears only when **Configure section terminology** is selected in the RAM form.<br>**Note:** Section label renaming applies only to the advanced risk assessment interface while leaving the terminology used in reports, dashboards, heatmaps, and other areas unchanged. | |
| Title | Option to rename the section title of the assessment type. For example, if you rename Residual assessment as Net assessment, the new title will be displayed in all sections where the Residual assessment was previously referred. |
| Score label | Option to rename the qualitative score label in the Scoring section of the assessment form. For example, if you rename Residual risk as Net risk, the new score label will be displayed in the scoring section where Residual risk was previously referred. |
| Annual loss expectancy label | Option to rename the quantitative score label in the Scoring section of the assessment form. For example, if you rename Residual ALE as Net ALE, the new score label will be displayed in the scoring section where Residual ALE was previously referred. |
| Heatmap Configuration | |
| This section appears only when the **Enable heatmap** option is selected. | |
| Factor for X-axis | Factor that appears on the X-axis of the heatmap. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Residual Assessment form (continued)**

| Field | Description |
|---|---|
| | **Note:** Only the qualitative factors of type **Choice** or factors with the transformation criteria can be selected. For more information, see Transformation criteria. |
| Factor for Y-axis | Factor that appears on the Y-axis of the heatmap.<br>**Note:** Only the qualitative factors of type **Choice** or with the transformation criteria can be selected. For more information, see Transformation criteria. |

### Configure a target assessment

Configure and publish a target assessment in the Advanced Risk application to assess your desired future risk level. By configuring a target assessment, you enable the assessors and approvers to perform a target risk assessment in the Next Experience.

#### Before you begin

Role required: sn_risk.admin

#### About this task

Configure a target assessment to assess the future risks levels. Similar to inherent and residual assessments, you can define the criteria for conducting target assessments. Configuration includes specifying factors, scoring logic, rating criteria, and heatmap configuration.

#### Procedure

1. Navigate to the Risk assessment methodology (RAM) form that has the target risk as an assessment type.
2. In the Assessment Types related list, select **Target Assessment**.
3. On the form, fill in the fields.

   For a description of the field values on the Target assessment form, see Target assessment form.

4. **Note:** If you selected **Factor responses** in the **Calculate based on** field, then you have to add factors to the assessment manually.

   To add factors, select the Factors related list and then do the following steps:

   a. Select **Edit**.

   b. Select the factors and add them to the Factors List.

   c. Select **Save**.

5. Optional: To add qualitative rating criteria, select the Qualitative Rating Criteria related list and select **New**.
6. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Qualitative Rating Criteria form**

| Field | Description |
|---|---|
| Lower rating interval | Range for the qualitative risk ratings. For example, for a range of 0–10, you can enter 0 as the lower range. For a range of 11– 20, the value can be 11 as the lower range. |
| Risk rating | Severity of the risk. You can enter ratings such as high, medium, or low. For example, assume that the lower rating interval for the Low rating is 0, and that the lower rating interval for the Medium rating is 11. If the risk score is 15, then the rating criterion is Medium because 15 is in the range of 11–20. |
| Overridden score | Score that the risk assessor can use to override the computed score. This score is associated with the risk when the rating is overridden. |
| Risk color style | Color code style for the background color on the risk rating value and for the text color on the risk assessment instance. For example, for a high risk, you can select the Red color style with the background color as red and the text as black. |
| Risk appetite scale | Risk appetite scale for the risk rating criteria. Appetite scales must be separately mapped to the qualitative risk rating criteria for Target Assessment in the RAM form. For example, you can select a risk appetite scale of **Hungry** for the risk rating of **Very High**. This field appears only when the risk appetite feature is configured in the advanced risk assessment properties. Future appetite status is calculated based on the defined risk appetite and the target risk profile.<br><br>**Note:** The future appetite status can't be aggregated or rolled up to any specific entities, risk statements, or individual risks. |

**Note:** Avoid entering negative values in the Qualitative Rating Criteria form.

7. Select **Submit**.
8. Optional: If you select the **Enable heatmap** option, you can do the following actions:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. To specify the risk color style, select the Heatmap Colors related list.

b. In the Risk color style column, specify the risk color style.

c. Select **Submit**.

9. To define the assessment result mapping for the applicable record types, do the following actions:

   These steps apply when conducting the target assessment on an object.

   a. Select the Assessment Result Mapping related list.
   The Assessment Result Mapping related list appears only when the **Update assessment results to source record** option is selected in the RAM.

   b. Select the record type.

   c. On the form, fill in the fields.

**Applicable Record Type form**

| Field | Description |
|---|---|
| Risk assessment methodology | Name of the RAM. This field is automatically set based on the selected RAM. |
| Record Type | Name of the applicable record type. This field is automatically set based on the selected record type. |
| Target risk rating | Column where the target risk rating value is stored in the source record. After the assessment, the target risk rating result is copied to the column that is selected in this field. This field appears only when the **Assessment contribution** field has **Qualitative** or **Both**. |
| Target ALE | Column where the target annual loss expectancy (ALE) value is stored in the source record. After the assessment, the target ALE result is copied to the column that is selected in this field. This field appears only when the **Assessment contribution** field is set to is **Quantitative** or **Both**. |

**Note:** If the same record type is used in another risk assessment methodology, the source record will update based on the field defined in the RAM of the latest advanced risk assessment.

   d. Select **Update**.

10. Select **Publish.**

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Target assessment form

Use the Target Assessment form in the Advanced Risk application to assess the desired future risk level in your organization.

See the following table for a description of the field values.

#### Target Assessment form

| Field | Description |
|---|---|
| Risk assessment methodology | Name of the RAM to which this target assessment belongs. This field is automatically set based on the selected RAM. |
| State | Current state of the assessment type. This field is automatically set to **Draft**. |
| Calculate based on | Options for calculating the assessment score:<br>• **Factor responses**: Option to select individual factors for the target assessment.<br>• **Factors same as inherent**: Option to copy the assessment contribution, scoring logic, and factors from the inherent assessment.<br>• **Factors same as residual**: Option to copy the assessment contribution, scoring logic, and factors from the residual assessment.<br>• **Overall assessment**: Option to continue without any factors selection. Assessors can directly provide rating or Annual loss expectancy (ALE) for the assessment. |
| Assessment contribution | Type of factor contribution:<br>• **Quantitative**<br>• **Qualitative**<br>• **Both**<br>**Note:** If **Factors same as inherent** or **Factors same as residual** is selected in the **Calculate based on** field, then **Assessment contribution** field is automatically set to a value defined in the inherent and residual assessment types. The field can't be modified. |
| Enable heatmap | Option to enable you to view the heatmap report on the Advanced Risk dashboard.<br>**Note:** This option can be selected only if a minimum of two factors are added to the assessment type. |
| Copy rating criteria from inherent | Option to copy the qualitative rating criteria from the inherent assessment. This option |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Target Assessment form (continued)**

| Field | Description |
|---|---|
| | appears only when the value **Factors same as inherent** is selected from the **Calculate based on** field. |
| Copy rating criteria from residual | Option to copy the qualitative rating criteria from the residual assessment. This option appears only when the value **Factors same as residual** is selected from the **Calculate based on** field. |
| Qualitative score | |
| This section appears only when the value **Qualitative** or **Both** is selected from the **Assessment contribution** field. | |
| Qualitative scoring logic | Formulae to calculate the qualitative scoring.<br><br>You can modify the **Qualitative scoring logic** field only when the value **Factor responses** is selected from the **Calculate based on** field. The options are as follows:<br><br>• **Sum**: Sum of the factor responses.<br>• **Minimum**: Minimum value of the factor responses.<br>• **Maximum**: Maximum value of the factor responses.<br>• **Average**: Average value of the factor responses.<br>• **Product**: Value derived by multiplying the factor responses.<br>• **Weighted average**: Average value of the weighting of factors. This value is then classified as low, medium, or high.<br>• **Script**: Use a custom script to calculate the qualitative score. The Script option enables you to create a customized calculation method that aligns with your organization's unique requirements and risk assessment approach. This option is available only to users with the sn_grc.developer role.<br><br>**Note:** Only users with the sn_grc.developer role can write or modify scripts for assessment types that aren't published. |
| Quantitative score | |
| This section appears only when the value **Quantitative** or **Both** is selected from the **Assessment contribution** field. | |
| Quantitative scoring logic | Formulae to calculate the quantitative scoring. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Target Assessment form (continued)**

| Field | Description |
|---|---|
| | You can modify the **Quantitative scoring logic** field only when the value **Factor responses** is selected from the **Calculate based on** field. The options are as follows:<br>• **Sum**: Sum of the factor responses.<br>• **Minimum**: Minimum value of the factor responses.<br>• **Maximum**: Maximum value of the factor responses.<br>• **Average**: Average value of the factor responses.<br>• **Product**: Value that is derived by multiplying the factor responses.<br>• **Script**: Use a custom script to calculate the quantitative score. The Script option enables you to create a customized calculation method that aligns with your organization's unique requirements and risk assessment approach.<br>**Note:** Only users with the sn_grc.developer role can write or modify scripts for assessment types that aren't published. |
| Section Labels | |
| This section appears only when the **Configure section terminology** option is selected in the RAM form.<br>**Note:** Section label renaming applies only to the advanced risk assessment interface while leaving the terminology used in reports, dashboards, heatmaps, and other areas unchanged. | |
| Title | Option to rename the section title of the assessment type. For example, if you rename Target assessment as Future assessment, the new title will be displayed in all sections where the Target assessment was previously referred. |
| Score label | Option to rename the qualitative score label in the Scoring section of the assessment form. For example, if you rename Target risk as Future risk, the new score label will be displayed in the scoring section where Target risk was previously referred. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Target Assessment form (continued)**

| Field | Description |
|---|---|
| Annual loss expectancy label | Option to rename the quantitative score label in the Scoring section of the assessment form. For example, if you rename Target ALE as Future ALE, the new score label will be displayed in the scoring section where Target ALE was previously referred. |
| Other Configurations | |
| Assessment is required | Option to make the target assessment either always required or conditionally required based on specific conditions. The options are as follows:<br>• **Always**: Option to make the target assessment required regardless of any specific conditions.<br>• **On specific conditions**: Option to make the target assessment required based on specific conditions using the condition builder.<br>• **On specific conditions specified through script**: Option to make the target assessment required using a predefined script or set of instructions. The Script option enables you to create a customized condition that align with your organization's unique requirements and risk assessment approach.<br>**Note:** Only users with the sn_grc.developer role can write or modify scripts. |
| Heatmap Configuration | |
| This section appears only when the **Enable heatmap** option is selected. | |
| Factor for X-axis | Factor that appears on the X-axis of the heatmap.<br>**Note:** Only the qualitative factors of type **Choice** or factors with the transformation criteria can be selected. For more information, see Transformation criteria. |
| Factor for Y-axis | Factor that appears on the Y-axis of the heatmap. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Target Assessment form (continued)**

| Field | Description |
|---|---|
| | **Note:** Only the qualitative factors of type **Choice** or with the transformation criteria can be selected. For more information, see Transformation criteria. |

### Create risk color styles

Create a library of risk color styles to use for different assessment types and matrixes. A risk color style is a combination of a background color and a text color. The color styles help maintain consistency when you configure risk assessments.

#### Before you begin
Role required: sn_risk.admin

#### About this task
ServiceNow® provides pre-configured color styles. You can either modify the pre-configured colors or create your own color styles.

#### Procedure
1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Risk Color Styles**.
2. Click **New**.
3. On the form, fill in the fields.

**Risk Color Style form**

| Field | Description |
|---|---|
| Color style | Name of the text and color code combination. For example, `High Risk`. |
| Background color | Color that appears as the background color. |
| Text color | Color that appears as the text color. |

4. Click **Submit**.

#### Result
The risk color style is ready for use.

### Configure risk heatmaps

Within a risk assessment methodology (RAM), configure the heatmap visualization for inherent and residual assessments. Use different heatmaps for different risk assessment methodologies.

#### Before you begin
Role required: sn_risk.admin

#### About this task
Configure the heatmap using the prepackaged heatmap widgets. Map the configured heatmaps to a dashboard to monitor the risk posture of the RAM.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to the dashboard where you want to add the heatmap.
2. In the upper-right corner, change the selected application from Global to GRC: Advanced Risk.
3. To add widgets, click the plus icon  in the upper right.
4. From the Add Widgets list, select one of the following.
   - **Advanced inherent heatmap**.
   - **Advanced residual heatmap** to configure the inherent heatmap or the residual heatmap respectively.
5. If you want to reuse an existing filter for the RAM, then do the following:

   a. Select **Interactive Filters** from the **Add Widgets** list

   b. Select **Reference**

   c. Select **Risk Assessment Methodologies**.
   Alternatively, you can create your own filter on the RAM table and add it on the dashboard tab.

### Result
The selected heatmap appears on the dashboard.

#### Create a risk assessment scope and initiate assessments

Create a risk assessment scope to define and identify risks for an entity. Identify assessors and approvers for assessments, and define the frequency of assessments.

### Before you begin
Role required: sn_risk.admin

### About this task
You can initiate assessments after you create the scope. This process provides visibility and accurate reporting for the management team.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Risk Assessment Scope** > **Create**.
2. On form, fill in the fields.

**Risk Assessment Scope form**

| Field | Description |
|---|---|
| Risk assessment methodology | Risk assessment methodology (RAM) that you use to assess risks. |
| Assessable Entity | Entities that are related to the entity classes that are selected in the **Applicable entity classes** field on the RAM. The value of this field changes based on the entity classes specified in your selected RAM. Only those entities that belong to the selected classes are displayed in this field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Owner | Owner of the entity. This field is automatically set based on the entity owner. |

3. Right-click and save the form.
4. Optional: To view a summary of assessments, click the Summary section.
   The Summary section has the following fields. These fields are populated only when you add risks to the assessment scope and when you initiate assessments:
   - **No. of risk assessments closed**
   - **No. of risks not assessed**
   - **No. of ongoing risk assessments**
5. Right-click to save the form.
6. If you want to add existing risks, then do the following:
   a. In the Risks related list, click **Add** to add existing risks.
   b. From the Choose Risks window, select the risks that you want to add.
   c. Click **Add Risks**.
   d. To select control objectives that do not have a control for the entity, click **Create from library**.
   e. From the Choose Risk Statements window, select what risk statements to apply and click **Create From Library**.
   f. Click **Initiate Assessments** either for all the risk records or for the selected risk records. Ensure that the selected records are in either the Draft or Closed state.
   g. To add new risks, click **New**, fill in the details, and click **Submit**.
   The newly added risks appear in the Risks related list.
7. To apply the new settings, click **Settings**.
8. On the form, fill in the fields.

### Assessor, approver, and frequency form

| Field | Description |
|---|---|
| Assessor type | User or group who is responsible for assessing the risk. Choices are the following:<br>◦ **Same as risk owner**<br>◦ **Specify users**<br>◦ **Specify groups**<br>◦ **Same as entity owner** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Assessor | User who is responsible for assessing the risk. This field appears only when **Specify users** is selected from the **Assessor type** field. |
| Assessor group | Group that is responsible for assessing the risk. This field appears only when **Specify groups** is selected from the **Assessor type** field. |
| Reassessment frequency | Frequency of assessment. Choices are the following:<br>◦ **None**<br>◦ **Weekly**<br>◦ **Monthly**<br>◦ **Quarterly**<br>◦ **Semi-annually**<br>◦ **Annually**<br>**Note:** If you need to perform an unplanned risk assessment before the next reassessment date, then the next assessment date will be based on the frequency set in the previous assessment. For example, if your frequency is set as monthly and you perform your first assessment on January1, and then you perform an unplanned assessment on January 15, then the next assessment will still be based on the previous assessment date. |
| Days to overdue | Number that is used to calculate the due date of the assessment starting from the date the assessment is initiated. For example, if the value in this field is 10, then the due date of the assessment will be 10 days after the date the assessment is initiated. The default value is 5. |
| Approver type | User or group who is responsible for approving the assessment. Choices are the following:<br>◦ **Same as entity owner**<br>◦ **Same as assessor's manager**<br>◦ **Specify users**<br>◦ **Specify groups**<br>◦ **None** |
| Approver | User who is responsible for approving the assessment. This field appears only when |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Specify users** is selected from the **Approver type** field. |
| Approver group | Group that is responsible for approving the assessment. This field appears only when **Specify groups** is selected from the **Approver type** field. |

The settings that you select in this step apply to all the new risks that are added to this scope.

9. To save the form, click **Submit**.
10. To generate the assessments, click **Initiate all assessments**.
    When you generate an assessment, the assessor receives an email notification stating that the assessment is assigned to the assessor or to the assessor's group.

### What to do next

If you want to cancel an assessment for risks that no longer need to be assessed, select the assessment and click **Cancel Assessments**.

**Note:** When a risk assessment is canceled, the risk assessors are notified about the cancellation and the tasks are removed from their queue.

## Simulate a risk assessment

Simulate a risk assessment to verify the associated risk assessment methodology (RAM) configuration when it is in the draft state.

### Before you begin

Role required: sn_risk.admin

### About this task

To modify the configuration of a published RAM, you need to delete all its assessments manually and change the RAM state to Draft. The simulation of risk assessment enables you to verify the RAM configuration when the RAM is in the draft state. This feature helps you to validate a factor, scoring logic, and the workflow and make necessary changes to the RAM before it is published. The simulated risk assessments are not used for risk aggregation and are deleted after the RAM is modified or published.

### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Administration** > **Risk Assessment Methodologies**.
2. Select and open the RAM for which you want to verify the configuration.

   **Important:** You should select a RAM that is in the draft state.

3. Click **Simulate**.

   **Important:** This button appears only when all the assessment types for the selected RAM are published.

   A dialog box appears for the risk or object selection.

4. Select a risk or object that you want to simulate.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Important:** You can select risks and objects that belong to the entity classes and tables specified in the RAM.

5. Click **Submit**.
   A simulated risk assessment is created, and a success message appears with the risk assessment number. You can click and open the risk assessment number to perform the assessment.
6. Optional: To view all the simulated assessments for the selected RAM, click **View simulated assessments**.

### Assess risks and objects on an assessment instance

Assess the risks that you have configured and reassign the risks to relevant approvers.

#### Before you begin

Role required: sn_grc.business_user

**Note:** You must manually assign the advanced risk assessment roles to the sn_grc.business_user role. To understand how you can adjust granting of roles and groups, see the How to adjust granting of roles and groups to use background jobs [KB0963693] article in the Now Support Knowledge Base.

#### Procedure

1. Navigate to **All** > **Advanced Risk Assessment** > **Risk Assessment Tasks** > **My Tasks**.
   The assessment is in the **Ready to assess** state.
2. To begin the assessment, click **Assess**.
   The work flow moves to the first risk assessment type. If a particular assessment type is not configured, then that section does not appear on the form.
3. Optional: To reassign an assessment, click **Reassign** and enter the name of the person who you want to reassign the assessment to.
4. Click the Inherent Assessment section and answer the questions on the form.

   a. Right-click and save the form.

   b. To move to the next assessment, click **Inherent Assessment** and fill in the fields.

#### Inherent Assessment section

| Field | Description |
|---|---|
| Results | |
| Computed inherent risk | Inherent risk score. |
| Override computed score | Option to override the computed inherent score. |
| Computed inherent ALE | Computed inherent ALE of the risk. The ALE is calculated based on the inherent assessment factors. |
| Override inherent risk | Value that was configured in the RAM form to override the computed inherent risk score. This field is available only when |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | the **Override computed score** option is selected. |
| Override inherent ALE | Value that overrides the computed inherent risk score. The value is used for rollup. |
| Comments | Additional information that provides more details for the risk assessment approver. Users must enter a reason for overriding the computed score. This field is required when the **Override computed score** option is selected. |

**c.** If necessary, add comments in the **Comments** column.

**d.** Click **Save and calculate**.

**5.** To perform control assessment, click **Perform control assessment** and do the following.

**a.** On the form, fill in the fields.

**Control Assessment section**

| Field | Description |
|---|---|
| Results | |
| Computed control effectiveness | Control effectiveness score. |
| Override computed score | Option for overriding the computed control effectiveness score. |
| Comments | Additional information that provides more details for the risk assessment approver. This field is required when the **Override computed score** option is selected. |

**Note:** If you have selected **Individual assessment of controls** in the **Calculate based on** field in the Control Assessment form, then you can create controls from the library, add existing controls, add new controls, or remove existing controls. Use guidance text for assistance in answering the factors. To determine if the control is compliant, see the Status column.

**b.** To create, add, or remove controls, perform one of the following actions:

| Choice | Action |
|---|---|
| To create controls from the library | **i.** Click **Create From Library** from the Choose Controls window.<br>**ii.** Select the necessary control objectives.<br>**iii.** Click **Add controls**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Choice | Action |
| --- | --- |
| To add an existing control | **i.** Click **Add**.<br>**ii.** Select the controls.<br>**iii.** Click **Add controls**. |
| To create a new control | **i.** Fill in the fields in the New Control window.<br>**ii.** Click **Submit**. |
| To remove any control | **i.** Click **Remove** from the Choose Controls window.<br>**ii.** Select the controls that you want to remove.<br>**iii.** Click **Remove controls**. |

If the risk has default controls, then those controls are automatically added to the control assessment.

**c.** If you do not have any controls that are associated with the risk or object that you must assess, then select the **No mitigating controls to assess** option.
If you choose not to assess the mitigating controls, then the residual risks are by default marked as not applicable in the residual assessment stage. However, if a risk has associated mitigating controls, then the users do not see the **No mitigating controls to assess** option.

**d.** If you opt out of assessing controls, enter a justification in the **Comments** field.

**e.** Click **Save and calculate**.

**6.** To move to the next assessment, click **Perform residual assessment** and do the following.

**a.** On the form, fill in the fields.

**Residual Assessment section**

| Field | Description |
| --- | --- |
| Results | |
| Computed residual risk | Residual risk score. |
| Comments | Additional information that provides more details for the risk assessment approver. This field is required when the **Override computed score** option is selected. |

**Note:** You can add existing controls and new controls during this stage. You can also remove controls that you might have wrongly added. The factors that appear for residual assessment are the factors that you have configured in the factor form. The answers that you provide for these factors determine the control assessment score. The score is based on the qualitative weight, qualitative score, and quantitative score.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

b. If you want to assess a residual risk but you have opted not to assess mitigating controls, then clear the **Residual risk not applicable** field.
If you do not want to assess a residual risk, then do not change the field.

c. Right-click and save the form.

7. To move to the next state and respond to the risks that you have assessed, click **Respond**.

a. In the **Risk Response** tab, click **Risk response** and select one or more risk responses from the following options:
   - **None**: Do not select any response for the risk.
   - **Accept**: Accept and acknowledge the risk.
   - **Avoid**: Eliminate the risk or its impact.
   - **Mitigate**: Lessen the impact or probability of the risk.
   - **Transfer**: Transfer the responsibility to a third party.

b. Right-click and save the form.

If multiple risk responses are selected, risk response tasks are created.

8. Click the Risk Response task related list, assign the task to an appropriate user, and right-click to save the form.
This related list only appears when the **Enable risk response** option is selected by the risk administrator during the RAM configuration.
9. In the **Comments** field, enter comments.
10. To view the activities for this assessment, click **Activity Journal**.
11. To finish your assessment and send it for approval, click **Save** and then click **Request Approval**.
The approver that you have selected in the risk assessment scope gets an email notification to approve or reject the risk assessment instance. If there are no approvers, the risk assessment instance moves to the Monitor state.

### What to do next
To view the summary of the assessment, click **Assessment Summary**.

## Assess risks

Use the classic risk assessment and assess the risks in your organization.

### Create a risk assessment using the Risk Assessment Designer

Use the Risk Assessment Designer to create and edit metric types, use different metric types for different risks, select multiple respondents for a risk assessment, as well as change scoring parameters. The Question Bank offers a library of questions for various categories, so you do not have to build each questionnaire from scratch.

### Before you begin
Role required: sn_risk.asmt_creator, sn_risk.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Risk** > **Administration** > **Assessment Types**.
2. Click **Risk Assessment Designer**.
   The designer contains the following elements:

| Element | Description |
|---|---|
| Controls | Supported question data types are available in the Controls palette. Drag a control onto the designer canvas to create a question of that type. |
| Questions | A library of questions for various categories, so you do not have to build each questionnaire from scratch. |
| Categories | New assessment open in the **Design** view. The questionnaire **Name** field appears above the first category in the canvas. A blank question field appears in the category container. |

3. Enter a name in the **Name** field.
4. Drag a control onto the designer canvas to create a question of that type.

#### Question controls

| Data type | Description | Scored |
|---|---|---|
| Attachment | Question with a Manage Attachments icon that allows users to attach one or more files. | Y |
| Boolean | Question with a check box or a **Yes/No** list for user responses. | |
| Choice | List of predefined options. For more information, see the definition for **Choices**. | Y |
| Date | Date field. | N |
| Date/Time | Date and time field. | N |
| Number | Number field with predefined minimum and maximum values. The default is 1-10. | N |
| Percentage | Percentage field with a prescribed range. | N |
| Scale | Predefined Likert scale. Answer options appear as radio buttons. | Y |
| Numeric Scale | Selectable number scale. The default is 1-5. Answer options appear as radio buttons. | Y |
| String | Single or multi-line text field. | N |
| Template | Choice list of templates that provide a predefined scale of options. | Y |
| Reference | Choice list of fields from a specified reference table. This data type does not support reference qualifiers. | |

**Note:** Set the correct answer for the metric that you want to be scored. Scored metrics determine the compliance status of the risk.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click one of the following tabs to change the view in the canvas.

| Option | Description |
|---|---|
| Design | Add categories and questions, and configure the properties of each. This is the default view of the canvas when you open the designer. |
| Configuration | Create introductions and end notes for attestations, and select a signature. |
| Availability | Select the recipients for each category in the attestation. |

6. Point to the menu icon in the upper right of the designer to select one of the following options.

**Note:** The availability of each option depends on the status of the assessment that is opened in the designer.

| Option | Description |
|---|---|
| Save | Save the current assessment. |
| Preview | Display a preview to the selected recipients. |
| Publish | Distributes the assessment to the selected recipients. |
| Save and Publish | Saves and distributes the assessment in one step. |
| New Attestation | Opens a fresh canvas for a new assessment. |
| Load Attestation | Opens a list of existing assessment that you can select and edit. |

Unlike other types of assessments, risk assessments do not appear in the **Self-Service** > **My assessments & surveys** module, because hundreds of control attestations could be generated at once. Instead,risk assessments are shown as a list in the **Risk** > **Risk Register** > **My Assessments** and **Risk** > **Risk Register** > **All Assessments** module.

### Create an assessment type

The risk manager can create a set of questions for each risk assessment.

#### Before you begin

Role required: sn_risk.asmt_creator or sn_risk.manager or sn_risk.administrator

#### Procedure

1. Navigate to **All** > **Risk** > **Administration** > **Assessment Types**.
2. Select **New**.
3. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Assessment Metric Type form

| Field | Description |
|---|---|
| Name | Name of the assessment type. |
| Assessment duration | Number of time assessors have to complete their assigned questionnaires, starting from the time the assessment is generated. |
| Table | Table that contains the records you want to evaluate. The system creates assessable records for records on this table that meet the conditions you specify, if any. The number of matching records appears as a link by the **Condition** field. If you change the table selection, the link dynamically updates. Select the link to open the list of matching records in a new tab or window.<br><br>**Note:** More roles are required to view the records on certain tables. If you select a table that you don't have access to, a warning message appears by the Condition field where the number of matching records would be. You can't generate assessable records for tables you don't have sufficient roles for. |
| Scale factor | Number to represent the best possible score for assessment results. All results for assessments of this type are scaled to this number. 10 is generally a good scale factor.<br><br>**Note:** This field becomes read-only when it contains a value and you save the metric type. Choose a scale factor that you're satisfied with before you save the metric type. |
| Condition | Condition builder that defines specific records to assess from the selected table. If you don't specify any conditions, the system creates assessable records for all records on the selected table. Select the refresh icon to update the adjacent record count.<br><br>**Note:** If you change the table or conditions, you must select **Generate Assessable Records** to create new assessable records. |
| Description | Helpful information about this type. Enter a clear description of the type and its purpose. |
| State | Status of the assessment: **Draft** or **Published**. |
| Enforce condition | Option that determines what happens to assessable records when you change the selected table or conditions. |
| Roles | Additional user roles that can view the results and access records associated with this type. Users with the specified roles have read access to this type record and to the associated categories, metrics, assessable records and scorecards, category users, stakeholders, and decision matrixes. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** Users with these roles don't have access to Assessments modules unless they're assessment administrators. Users with these roles can navigate to the records by other means, such as from reference fields on assessment instances. This field provides the option to grant user access to specific assessment data in special cases. For example, the Vendor metric type provides access to users with the vendor_manager role to view results and compare assessable records when they open scorecards or decision matrixes in the Vendor Performance application. |

4. Select **Submit**.

### Assess risk for a policy exception

After the review of a policy exception request and before deciding to approve or reject a request, the compliance manager may choose to request a risk assessment by the risk manager.

## Before you begin

Role required: compliance manager

## About this task

For more information, see Manage policy exceptions and extensions.

## Procedure

1. Navigate to **All** > **Policy and Compliance** > **My Policy Exceptions**.
2. Select the policy exception.
3. Review the form details, as necessary.
4. Click the Business Impact Analysis tab and update the following fields:

**Policy exception request Business Impact Analysis tab**

| Field | Value |
| --- | --- |
| Risk description | Description of the risk. |
| Residual likelihood | Likelihood of the risk occurring. If it is not **None**, select the likelihood of this risk occurring:<br>◦ **5 — Extremely Likely**<br>◦ **4 — Likely**<br>◦ **3 — Neutral**<br>◦ **2 — Unlikely**<br>◦ **1 — Extremely Unlikely** |
| Residual impact | Residual impact of the risk. If it is not **None**, select the residual impact of this risk:<br>◦ **5 — Very High**<br>◦ **4 — High**<br>◦ **3 — Moderate** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Value |
|---|---|
| | ◦ **2 — Low**<br>◦ **1 — Very Low** |
| Residual score | Value calculated after you select a residual likelihood and residual impact rating:<br>◦ **5 — Very High**<br>◦ **4 — High**<br>◦ **3 — Moderate**<br>◦ **2 — Low**<br>◦ **1 — Very Low** |

5. Perform one of the following actions.

| Option | Action |
|---|---|
| To view or add impacted controls to the policy exception | **a.** Click the Impacted Controls tab.<br>**b.** Click **Add** or **Add All**.<br>**c.** Choose the controls to associate to the policy exception. |
| To view mitigating controls on the policy exception | Click the Mitigating Controls tab. |
| To view or add risks to the policy exception | Click the Risks tab.<br>**Note:** This option is available when Governance, Risk, and Compliance is also activated. |
| To view or add approvers to the policy exception | Click the Approvers tab. |
| To view or add task service level agreements to the policy exception | Click the Task SLAs tab. |

6. Click **Update**.

### Assess a risk

Risks start in a **Draft** state then move to the **Assess** state.

### Before you begin

Role required: sn_grc.user

### About this task

Risk assessments do not appear in the **Self-Service** > **My assessments & surveys** module, because hundreds of GRC assessment records could be generated at once. Instead, risk assessments are shown in a separate list view.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Register** > **My Assessments**.
2. Open the assessment and review the details.

| Option | Description |
|---|---|
| If you are unable to answer the questions | **a.** Reassign the assessment to another user in the **Assigned to** field.<br>**b.** Click **Update** and close the record.<br>**Note:** Only a user with the sn_grc.user role can be re-assigned the assessment.<br>The list of assessments refreshes when you reassign an assessment to another user. |
| If you are able to answer the questions | **a.** Click **Take assessment**.<br>**b.** Answer the questions and attach information, as required.<br>**c.** Click **Submit**.<br>The list of assessments refreshes when you close the **Take Assessment** pop-up window. |

## Manage a business process

Create and manage business processes in your organization.

### Create a business process

Create a business process and define the owners, approvers, business criticality, and review frequency for the process.

### Before you begin

Role required: business_process_admin

### Procedure

1. Navigate to **All** > **CSDM** > **Design** > **Business Process**.
2. Click **New**.
3. On the form, fill in the fields.

#### Business Process form

| Field | Description |
|---|---|
| Name | Name of the business process. |
| Parent | Parent business process. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** If a parent process exists, it creates a hierarchy of business processes. |
| Life cycle stage | Stage of the business process in the business life cycle. The stage determines the status and displays the actions.<br>**Note:** This field is automatically set to **Ideation** when you save the form for a process in the Draft state. |
| Review frequency | Frequency for reviewing the business process. |
| Life cycle stage status | Status of the business process within the life-cycle stages.<br>**Note:** This field is automatically set to **Under Evaluation** when you save the form for a process in the Draft state. |
| Next review date | Planned date on which the business process must be reviewed. The value in this field is automatically set only after the business process is approved. |
| Description | Short description of the business process. The description can include the background, the actual steps, and the interaction of the process. |
| Ownership | |
| Managed by group | Group that maintains the business process. |
| Approval group | Group that must review and approve the business process. |
| Owned by | User responsible for the business process. This user is a member of the Managed by group. |
| Business Impact | |
| Business criticality declared | Criticality of the business process based on your subjective assessment. The choices are:<br>◦ **1- most critical**<br>◦ **2- somewhat critical**<br>◦ **3- less critical**<br>◦ **4- not critical** |
| Impact to confidentiality | Risk rating for the risk of loss of confidentiality. Confidentiality loss leads to leakage of confidential information. The choices are the following: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ **High**<br>◦ **Medium**<br>◦ **Low** |
| Impact to availability | Risk rating for the risk of loss of availability. Unavailability of the system may cause delays in decision making, business interruptions, loss of revenue, and customer dissatisfaction. The choices are the following:<br>◦ **High**<br>◦ **Medium**<br>◦ **Low** |
| Business criticality determined | Computed criticality of the business process based on the assessment of the subprocesses. The choices are the following:<br>◦ **1- most critical**<br>◦ **2- somewhat critical**<br>◦ **3- less critical**<br>◦ **4- not critical** |
| Impact to integrity | Risk rating for the risk of impact to integrity. Impact to integrity has consequences for businesses and employees, including fines and damage to your brand, reputation, and people. The choices are the following:<br>◦ **High**<br>◦ **Medium**<br>◦ **Low** |

4. Right-click on the form header and click **Save**.
   The record moves to the Draft state.
5. To send the record for review and approval, click **Review**.
   The values in the **Life cycle stage** field and the **Life cycle stage status** field change. The Approvals related list appears, and the members of the Approval list can view the record in their list of approvals.

### Approve, reject, or delete a business process

If a new business process has identified approvers, then the approvers must review and approve the process before it can be published. The approvers can also reject or delete the process as necessary.

**Before you begin**
Role required: business_process_manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **Service Desk** > **My Approvals**.
2. Open the record that you want to approve.
3. In the **State** field, select one of the following options:
   - Not Yet Requested
   - Requested
   - Approved
   - Rejected
   - Canceled
   - No Longer Required
4. In the **Comments** field, enter your comments as required.
   If the reviewer rejects the record, then the reviewer must enter comments.
5. Select one of the following options.

| Option | Description |
|---|---|
| Approve | Approve the business process. If you select this option, the business process is published. |
| Reject | Reject the business process. If you select this option, the business process moves back to the Draft state. |
| Delete | Delete the business process. |

## Create a risk framework and associate risk statements to it

Risk managers create risk frameworks to group risk statements into manageable categories.

### Before you begin

Role required: sn_risk.manager

### Procedure

1. Navigate to **All** > **Risk** > **Risk Library** > **Frameworks**.
2. Click **New**.
3. On the form, fill in the fields.

#### Risk Framework form

| Field | Description |
|---|---|
| Number | Read-only field that is automatically populated with a unique identification number. |
| Active | Option that indicates whether the risk framework is active. |
| Name | The name of the risk framework. |
| Description | A description of the risk framework. |
| Additional information | Additional information for this risk framework. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Click **Submit**.
5. Select the risk framework from the list to reopen it.
6. In the **Risk Statements** related list, select **Edit** to add the risk statements to the risk framework.
7. Click **Save**.

## Define risk statement hierarchy

Risk managers establish parent and child relationships on the risk statement form.

### Before you begin

Role required: sn_risk.manager

### Procedure

1. Navigate to **All** > **Risk** > **Risk Library** > **Risk Statements**.
2. Click **New**.
3. On the form, fill in the fields.

**Note:** When any of the following statement fields changes: Name, Description, Reference, Category, Type, Classification, and Attestation, all the associated controls and risks are updated, and their state is set back to Draft.

**Risk Statement from**

| Field | Description |
|---|---|
| Name | Name of the risk statement. |
| Parent * this field is visible only when Advanced Risk has been downloaded. | Parent risk statement to this risk statement.<br>◦ Users select the appropriate parent from the taxonomy structure.<br>◦ If no parent is specified, the risk statement becomes the root of the tree.<br>◦ It is possible to have several of these root-type risk statements within the organization.<br>◦ A risk statement cannot be both a parent and a child of another risk statement. |
| Framework | Framework this risk statement is associated with. |
| Category | Choose a category.<br>◦ Legal<br>◦ Financial<br>◦ Operational<br>◦ Reputational<br>◦ Legal/Regulatory<br>◦ Credit<br>◦ Market<br>◦ IT |

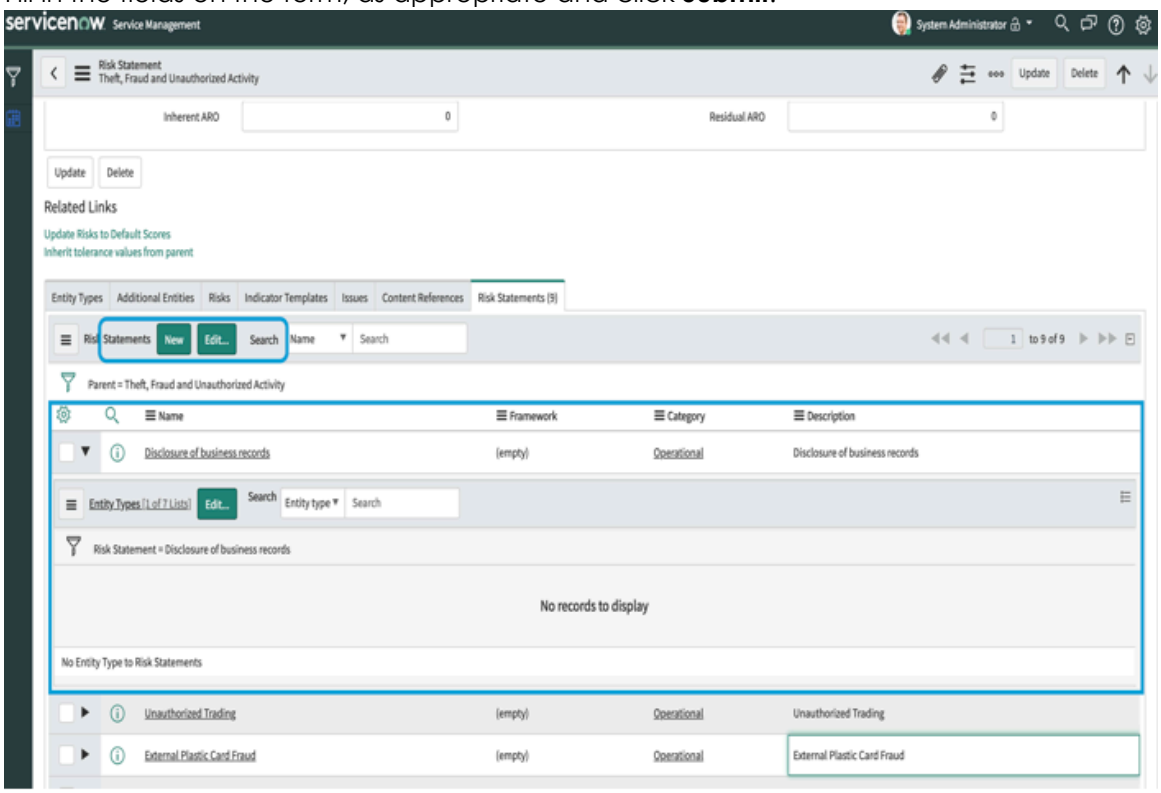
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Assessment | Assessment associated with this risk statement. |
| Issue group rule | Issue group rule assigned to this risk statement for reporting and dashboard. |
| Description | Description of the risk statement. |
| Additional information | Additional information for this risk statement. |
| Default Scores | |
| Inherent SLE | Monetary value of a risk if it occurs before any mitigation strategies are in place. |
| Residual SLE | Monetary value of a risk if it occurs after all mitigation strategies are in place. |
| Inherent ARO | Probability that a risk occurs in any given year before any mitigation strategies are in place. |
| Residual ARO | Probability that a risk will occur in any given year after all mitigation strategies are in place. |
| Risk Rollup and Tolerance * this tab is visible only when Advanced Risk has been downloaded. | |
| Expected ALE | Enter currency and amount for the expected ALE.<br>**Note:** This value must be less than or equal to the **Maximum acceptable ALE**. |
| Maximum acceptable ALE | Enter currency and amount for the maximum acceptable ALE.<br>**Note:** This value must be greater than or equal to the**Expected ALE**. |
| Sum of calculated ALE | This is a calculation based on all the underlying risks or risk statements. |
| Average calculated ALE | This is a calculation based on all the underlying risks or risk statements. |
| Maximum calculated ALE | This is a calculation based on all the underlying risks or risk statements. |
| Minimum calculated ALE | This is a calculation based on all the underlying risks or risk statements. |
| Tolerance Status | Automatically calculated based on tolerance values.<br>◦ If the **Calculated ALE** is less than or equal to the **Expected ALE** = Acceptable in green<br>◦ If the **Calculated ALE** is greater than the **Expected ALE**, but less than or equal to the **Max acceptable ALE** = Needs Attention in orange<br>◦ If the **Calculated ALE** is greater than the **Maximum acceptable ALE** = Unacceptable in red |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Calculated Score | The corresponding score for the calculated ALE:<br>◦ Low<br>◦ Med<br>◦ High |

4. Click **Submit**.
5. To add children risk statements, click the **Risk Statements** related list, and click **New**.
6. Fill in the fields on the form, as appropriate and click **Submit**.




7. Repeat until you have added all the children risk statements related to this risk statement.

## Create a risk statement

Risk managers create risk statements to group risks into manageable categories.

### Before you begin

Role required: sn_risk.manager

### Procedure

1. Navigate to **All** > **Risk** > **Risk Library** > **Risk Statements**.
2. Click **New**.
3. On the form, fill in the fields.

> **Note:** When any of the following statement fields changes: Name, Description, Reference, Category, Type, Classification, and Attestation, all the associated controls and risks are updated, and their state is set back to Draft.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk Statement form**

| Field | Description |
|---|---|
| Name | Name of the risk statement. |
| Parent | Parent risk statement. |
| Framework | Framework this risk statement is associated with. |
| Category | Choose a category.<br>◦ Legal<br>◦ Financial<br>◦ Operational<br>◦ Reputational<br>◦ Legal/Regulatory<br>◦ Credit<br>◦ Market<br>◦ IT |
| Assessment | Risk assessment template to be assigned to this risk statement. An assessment template is a questionnaire that is used for assessing a risk. |
| Description | Description of the risk statement. |
| Additional information | Additional information for this risk statement. |

**Note:** Accurate default scoring selections are important for normalizing risk across the organization.

4. To fill in the fields for the risk appetite section, see Define the risk appetite for a risk statement.
5. Click the **Default Scores** related list and fill in the fields on the form, as appropriate.

**Default Scores form**

| Field | Description |
|---|---|
| Inherent SLE | Impact that the event has on the organization if there are no controls to check the event. |
| Residual SLE | Impact that the event has on the organization if there are controls to check the event. |
| Inherent ARO | Likelihood of the event occurring if there are no controls to check the event. |
| Residual ARO | Likelihood of the event occurring if there are controls to check the event. |

6. Click the **Risk Rollup and Tolerance** related list and on the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk Rollup and Tolerance form**

| Field | Description |
|---|---|
| Expected ALE | Annual Loss of Expectancy (ALE) refers to the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). Expected ALE is the expected value of the ALE for the risk statement. Enter currency and amount for the expected ALE.<br>**Note:** This value must be less than or equal to the **Maximum acceptable ALE**. |
| Sum of calculated ALE | This calculation is based on the sum of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Maximum calculated ALE | This calculation is based on the maximum of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Maximum acceptable ALE | Threshold value for the ALE for the risk statement.<br>**Note:** This value must be greater than or equal to the**Expected ALE**. This value has an impact on the Tolerance status field. |
| Average calculated ALE | This calculation is based on the average of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Minimum calculated ALE | This calculation is based on the minimum of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Calculated Score | The corresponding score for the calculated ALE:<br>◦ Low<br>◦ Med<br>◦ High |

7. Click the **Basel Categorization** related list and select the Basel Categories Hierarchy. The Basel categories are as follows:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Internal Fraud: misappropriation of assets, tax evasion, intentional mismarking of positions, bribery.
- External Fraud: theft of information, hacking damage, third-party theft and forgery.
- Employment Practices and Workplace Safety: discrimination, workers compensation, employee health and safety.
- Clients, Products, and Business Practice: market manipulation, antitrust, improper trade, product defects, breaches, account churning.
- Damage to Physical Assets: natural disasters, terrorism, vandalism.
- Business Disruption and Systems Failures: utility disruptions, software failures, hardware failures.
- Execution, Delivery, and Process Management: data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets.

8. Click **Submit**.

## Visualize risk hierarchies using the GRC: Workbench

Risk users can see the hierarchy of risk statements using the GRC: Workbench.

### Before you begin

Activate the GRC: Workbench (app-grc-workbench) plugin.

Role required: sn_risk.reader

### Procedure

1. Navigate to **All** > **Risk** > **GRC Workbench**.
2. Click **Risk Dependencies**.
3. Click **Risk Statement Hierarchy**.
4. On the left pane, click the risk statement for which you want to visualize the risk statement hierarchy.

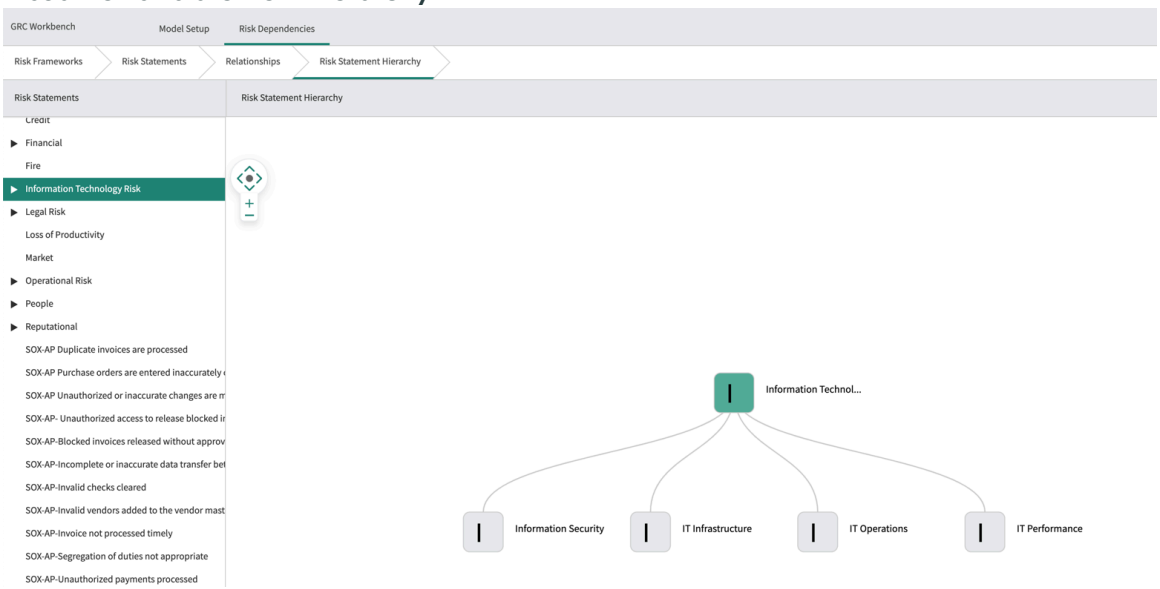
   **Example**

   For example, if you want to see the hierarchy of the Information Technology risk statement, click Information Technology Risk and you can see the parent risk statement and the child risk statements such as information security, IT infrastructure, IT operations, and IT performance.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The risk statement hierarchy is displayed.

**Visualize risk statement hierarchy**




## Generate a risk from a risk framework

Making associations with risk frameworks automatically creates risks.

### Before you begin

Role required: sn_risk.admin and sn_risk.manager

### Procedure

1. Navigate to **All** > **Risk** > **Risk Library** > **Risk Framework**.
2. Open the risk framework record.
3. In the **Entity Type** related list, click **Edit**.
4. Select the entity types to associate to the risk framework, and click **Save**.
   All risk statements are associated to the entity type and a risk is created for every risk statement against every entity in the entity type.

## Generate a risk from a risk statement

Making associations with risk statements automatically creates risks.

### Before you begin

Role required: sn_risk.admin and sn_risk.manager

### Procedure

1. Navigate to **All** > **Risk** > **Risk Library** > **Risk Statement**.
2. Open the risk statement record.
3. In the **Entity Type** related list, click **Edit**.
4. Select the entity types to associate to the risk statement, and click **Save**.
   One risk is generated for each entity in the entity type based on the risk statement.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Relate risks to each other

Create relationships between risks to better understand how risks affect each other and how they affect the enterprise.

### Before you begin

Role required: sn_risk.manager or sn_risk.admin

### Procedure

1. Navigate to **All** > **Risk** > **Risk Register** > **All Risks**.
2. Open a risk.
3. Perform one of the following actions.

| Option | Description |
|---|---|
| To specify that the current risk is down-stream of another risk | Click the **Add** button in the **Upstream Risks** related list. |
| To specify that the current risk is upstream of another risk | Click the **Add** button in the **Downstream Risks** related list |

4. Select the desired risks to relate to the current risk and click **Create Relationship**.
5. In the pop-up window, check all the desired risks to relate to the current risk, and click **Create Relationship**.

## Create a risk manually

Risk administrators can create risk records when they see a potential for a gain or loss of value.

### Before you begin

Role required: sn_risk.user

### Procedure

1. Navigate to **All** > **Risk** > **Risk Register** > **Create New**.
2. On the form, fill in the fields.

**Risk form**

| Field | Description |
|---|---|
| Number | Unique identification number. This field automatically populated. |
| Inherit from risk statement | Option to create a risk independent of risk statement. |
| Active | Option to indicate if the risk is active. |
| Name | Name for the risk. Field is auto-populated if the risk is generated from a risk statement, but can be changed without affecting the relationship between the risk and risk statement. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Description | Description of the risk and how it is a threat to the organization. |
| Risk Statement | Risk statement this risk is associated with. |
| Category | Category of risk which applies to the profile.<br>◦ Legal<br>◦ Financial<br>◦ Operational<br>◦ Reputational<br>◦ Legal/Regulatory<br>◦ Credit<br>◦ Market<br>◦ IT<br>If the risk is generated from a risk statement, the field is automatically populated/ |
| Entity | Entity related to the risk.<br>**Note:** Only active entities are shown. |
| Owning group | Owning group for the risk. |
| Risk relevance | Explanation of how this risk applies to you.<br>**Note:** This field only appears when the **Inherit from risk statement** option is selected. |
| Owner | Owner for the risk.<br>**Note:** The owner is always added as a respondent. |

3. Click the **Assessment Summary** tab.
   This tab is only visible if you have the Advanced Risk plugin activated. The scores of the risk assessment methodology selected as the primary are displayed in the risk scoring section. If the Advanced Risk plugin is not activated, then the following sections for classic risk appear.
4. To fill in the fields for the risk appetite section, see Define the risk appetite for a risk.
5. On the form, fill in the fields.

**Risk Scoring Form**

| Field | Description |
|---|---|
| **Note:** These fields appear for classic risk. | |
| Assessment | Assessment to attach to this risk. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** If you are defining this risk for a Data Protection Impact Assessment (DPIA), select GDPR DPIA Assessment. |
| Assessment respondents | Users assigned to the assessment of this risk.<br>**Note:** Only a user with the sn_grc.user role can be added as a respondent. |

When both the **Assessment** and **Assessment respondents** fields are set, assessments are created when you click **Assess**.

6. Click the **Scoring** tab.
7. On the form, fill in the fields.

**Risk Scoring form**

| Field | Description |
|---|---|
| **Note:** These fields appear for classic risk. | |
| Inherent SLE | Monetary value of a risk if it occurs before any mitigation strategies are in place. |
| Residual SLE | Monetary value of a risk if it occurs after all mitigation strategies are in place. |
| Inherent ARO | Probability that a risk occurs in any given year before any mitigation strategies are in place. |
| Residual ARO | Probability that a risk will occur in any given year after all mitigation strategies are in place. |
| Inherent ALE | Annualized loss expectancy `ALE = SLE x ARO` before any mitigation strategies are in place. |
| Residual ALE | Annualized loss expectancy `ALE = SLE x ARO` after all mitigation strategies are in place. |
| Inherent score | The score of the risk before any mitigation strategies are in place. |
| Residual score | The score of the risk after all mitigation strategies are in place. |
| Calculated ALE | Annualized loss expectancy based off all calculations. |
| Calculated score | The corresponding score for the calculated ALE. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Click the **Response** tab.
9. On the form, fill in the fields.

**Risk Response form**

| Field | Description |
|---|---|
| Response | ◦ Accept<br>◦ Avoid<br>◦ Mitigate<br>◦ Transfer |
| Justification | Enter a reasonable justification for the selected response |

10. Click the **Monitoring** tab.

**Risk Monitoring form**

| Field | Description |
|---|---|
| Control compliance percentage | Percentage of compliant controls |
| Control non-compliance percentage | Percentage of non-compliant controls |
| Control failure factor | Sum of failed controls weighting divided by total controls weighting |
| Indicator failure factor | Uses the last result of each associated indicator. Number of last results failed divided by total number of indicators associated. |
| Calculated risk factor | This value is calculated from `(Indicator failure factor + Control failure factor) / 2`. |

11. Click the **Activity Journal** tab.
12. Enter additional comments, as necessary.
13. Click **Submit**.

## Follow a risk

Connect integrates with Risk Management providing an overlay to the standard interface, allowing users to participate in conversations while they work and collaborate on the risk record.

### Before you begin

Role required: sn_risk.user
For more information about Connect, see Connect.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Register** > **All Risks**.
2. Open the risk record from the list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click the **Follow** tab and perform one of the following actions.

| Option | Action |
|---|---|
| To add the Connect sidebar | Click **Open Connect mini**. |
| To add the Connect full-screen view | Click **Open Connect Full**. |

## Add a control to a risk

Controls are added to the risks for the on-going review of processes.

### Before you begin

Role required: sn_risk.manager and sn_compliance.manager

### About this task

### Procedure

1. Navigate to **All** > **Risk** > **Risk Register** > **All Risks**
2. Open the risk record from the list.
3. Continue with one of the following options.

| Option | Description |
|---|---|
| Add an existing control | **a.** In the **Controls** related list, select **Add**.<br>**b.** Select the controls that are associated with the risk profile.<br>**c.** Select **Add relationship**.<br>**Note:** The controls displayed after selecting the **Add** button are limited to controls where the entity of control matches the risk entity. If there are no eligible controls that can be related to the risk, the **Add** button isn't displayed on the Controls related list. |
| Add a new control | **a.** In the **Controls** related list, select **New**.<br>**b.** On the form, fill in the fields. For a description of the field values on the Control form, see Create a control.<br>**c.** Select **Submit**. |
| Inherit common controls | **a.** In the **Controls** related list, select **Inherit common controls**.<br>**b.** Select the controls.<br>**c.** Select **Add**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| | **Note:** The common controls displayed after selecting the **Inherit common controls** button are limited to controls where the reliant entity of control matches the risk entity. If there are no eligible controls that can be related to the risk, the **Inherit common controls** button isn't displayed on the **Controls** related list. |

- When a control objective and risk statement are associated and the control entity matches the risk entity, the risk-control association is created.
- The risks and controls that are created after associating a control objective to the risk statement aren't associated with the risk statement immediately. They get associated when the *GRC Profile Generation* scheduled job runs.
- If you manually delete a control from a risk, the control won't be re-created by the scheduled job. You must manually create it again if necessary.

Related topics

Associate a risk statement with a control objective in the Risk Workspace

## Manually create GRC issues

As a GRC user, you can manually create issues to document policy, risk, or audit observations, or to accept any GRC problems. You can also identify the source of the issue to help analyze and classify the issues.

### Before you begin

Role required: (per product)

- In Policy and Compliance Management: compliance_admin, compliance_manager, sn_compliance.user, sn_grc.business_user, sn_grc.business_user_lite
- In Risk Management: risk_admin, risk_manager, or sn_risk.user
- In Audit Management: audit_admin, audit_manager, audit_admin, or sn_audit.user

**Note:** Starting with Version 12.0.1 of the products mentioned above, the minimum role for the **Assigned to** user on the Issues form is GRC Business User [sn_grc.business_user]. The minimum role for the **Issue manager** is GRC User [sn_grc._user].

For more information on the access control limitations to issues, see GRC business user role to control access and track usage of compliance tables.

### Procedure

1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Issues** > **Create New**.
   - **Risk** > **Issues** > **Create New**.
   - **Audit** > **Issues** > **Create New**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** Starting with Version 12.0.1 of the products mentioned above, the minimum role for the **Assigned to** user on the Issues form is GRC Business User [sn_grc.business_user]. The minimum role for the **Issue manager** is GRC User [sn_grc._user].

2. On the form, fill in the fields.

**Issue form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Assignment group | Group to which this issue has been assigned. Each member gets a notification when an activity happens on this issue. |
| Assigned to | Member of the group assigned to resolve the issue.<br><br>Starting with Version 12.0.1, the user must have at least the sn_grc.business_user role.<br><br>**Note:** Use the bulb icon to get suggestions on who must the issue be assigned to. The bulb icon only appears if you have the GRC: Predictive Intelligence application activated, the form is saved, the **Assigned to** field is not inactive, and the GRC Property is selected as Similarity Analysis. For more information, see .<br><br>You can configure a hierarchy of users to access the issue record. For more information, see User hierarchy access control for issue and remediation task records.<br><br>Starting with Version 12.0.1, the assigned-to user gets an email notification when the issue manager requests more information.<br><br>Starting with Version 12.0.1, when an issue transitions to the **Respond** state, an entry in the **Assigned to** field is mandatory. |
| Issue source | Source from where the issue was created. This field is auto-populated with one of the following options based on how the issue is created:<br>◦ Indicator Failure: Issue is created by a failure of the indicator<br>◦ Risk Assessment: Issue is created in a risk<br>◦ Risk Event: Issue is created in a risk event |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Control Attestation Failure: Issue is created due to a non-compliant control<br>◦ Control Test Failure: Issue is created when a control is ineffective and the control test is marked as closed and complete<br>◦ Ad-hoc: Issue is manually created |
| Issue type | Type of issue. Choices are:<br>◦ Control design effectiveness failure<br>◦ Control operative effectiveness failure<br>◦ Control does not meet requirement<br>◦ Control does not exist<br>◦ Non-compliance to a regulation<br>◦ Non-compliance to a policy<br>◦ Improvement or suggestion to an existing policy<br>◦ Recommendation for a new policy<br>◦ Process optimization or improvement<br>◦ Observation<br>◦ Data Breach<br>◦ Fraud<br>◦ Misstatement<br>◦ Training<br>◦ Documentation<br>◦ Risk issue<br>◦ Other |
| Classification | The classification of the issue as a risk, compliance, or audit, based on the issue type. |
| Issue manager group | The group responsible for managing and reviewing the issue.<br>Starting with Version 12.0.1, the following enhancements and requirements were introduced:<br>◦ Members of the issue manager group must have one of the following roles:<br>▪ sn_audit.manager<br>▪ sn_audit.user<br>▪ sn_compliance.manager<br>▪ sn_compliance.user<br>▪ sn_grc.manager |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ▪ sn_grc.user<br>▪ sn_risk.manager<br>▪ sn_risk.user<br>◦ When an issue transitions to the **Analyze** state, an entry in either the **Issue manager group** or **Issue manager** field is mandatory.<br>◦ When an issue is assigned to the group, the members receive an email notification. Additionally, the issue manager receives an email notification when the issue transitions to the **Review** state. |
| Issue manager | The user responsible for managing and reviewing the issue.<br>Starting with Version 12.0.1, the following enhancements and requirements were introduced:<br>◦ The issue manager must have at least the sn_grc.user role.<br>◦ The issue manager receives an email notification when the assigned-to user provides requested information.<br>◦ When an issue transitions to the **Analyze** state, an entry in either this field or **Issue manager** is mandatory.<br>◦ When an issue transitions to the **Respond** state, an entry in this field is mandatory. |
| State | ◦ New<br>◦ Analyze<br>◦ Respond<br>◦ Review<br>◦ Closed Complete<br>◦ Closed Incomplete |
| Substate | The substate and applicable details for the substate. |
| Priority | The sequence in which an issue must be resolved, based on its impact and urgency:<br>◦ **1 — Critical**<br>◦ **2 — High**<br>◦ **3 — Moderate**<br>◦ **4 — Low**<br>◦ **5 — Planning** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Issue rating | Starting with Version 12.0.1, the issue manager can assign the issue rating to the issue. Based on the issue rating, the **Due date** under the **Dates** tab is calculated as follows and displayed:<br>◦ Very high (2 days)<br>◦ High (4 days)<br>◦ Moderate (8 days)<br>◦ Low (10 days)<br>◦ Very Low (15 days)<br>You can manually override the **Due date**.<br>**Note:** Users with the sn_grc.manager and sn_grc_advanced.issue_triage_manager role can navigate to **Policy and Compliance** > **Administration** > **Issue rating** and define additional issue ratings.p<br>When the issue transitions to the **Respond** state, the Issue rating field is read only. |
| Issue group rule | Group rule assigned to this issue. The Issue group rule is used to group similar issues together into a parent issue based on the conditions defined in the rule. This rule enables you to work on similar issues simultaneously and close out the parent issue after all issues are resolved. This closes out all the child issues. |
| Parent Issue | Parent issue this issue belongs to. |
| Configuration item | Item associated with this issue. If all child issues have the same configuration item, it gets copied over to the parent issue |
| Location | Location where the issue occurred. |
| Short description<br>Starting with Version 12.0.1, this label was changed to **Name**. | A name for the issue. |
| Description | A more comprehensive description of the issue. |
| Details | |
| Control/Risk | Control or risk associated with the issue.<br>When the control is associated, the corresponding entity of the control |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | is added to the **Entity** field, and the control objective is added to the **Control Objective/Risk Statement** field. These control objective and entity are the ones that are linked to this control.<br><br>When the control is associated to the issue form, an m2m record is created in the source [sn_grc_m2m_issue_item] table. Whenever a record is added in the source table, a corresponding record, Issue to Entity is added in the destination [sn_grc_m2m_issue_to_entity] table, and another record Issue to Content is added in the destination [sn_grc_m2m_issue_content] table for the associated entity and control objective of the control. |
| Entity | Related entity. |
| Policy | The policy associated with the issue. |
| Authority document | The authority document associated with the issue. |
| Control Objective/Risk Statement | The control objective or risk statement related to this issue. |
| Recommendation | Resolution actions recommended by the risk, compliance, or audit teams. |
| Action Plan | The plan for remediating the issue. |
| Dates | |
| Planned start date | Date and time that work on the issue is expected to begin. |
| Planned end date | Date and time that work on the issue is expected to end. |
| Planned duration | Estimated amount of work time for the issue. |
| Confirmed date | (Starting with Version 12.0.1) The date when the issue is confirmed. This field is read-only, and displays today's date when the issue is moved from **New** to any of the following states:<br>◦ **Analyze**<br>◦ **Review**<br>◦ **Respond**<br><br>**Note:** If a triage issue is converted to an actual issue, this field displays the date it was converted. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Due date | (Starting with Version 12.0.1) This date is auto-populated based on a GRC property. Navigate to **Policy and Compliance** > **Administration** > **GRC Properties**. If the **Auto populate due date based on issue rating** property is set to **Yes**, this field is auto-populated based on the predefined remediation time frame for the issue's risk rating. Otherwise, you can manually enter a due date.<br><br>When an issue transitions to the **Respond** state, an entry in this field is mandatory. |
| Actual start date | Time when work began on this issue. |
| Actual end date | A read-only value that is determined by the **Actual duration** input field. |
| Actual duration | Amount of work time. |
| Created | The date and time the issue was created. |
| Closed | The date and time the issue was closed. |
| Engagement | |
| Engagement | The related engagement. |
| Activity | |
| Additional comments (Customer visible) | Public information about the issue. Click **Post** to add your comments to the issue. |
| Work notes | Click the **Work notes** check box to display the **Work notes** field. Information about how to resolve the issue, or steps already taken to resolve it, if applicable. Work notes are visible to users who are assigned to the issue. Click **Post** to add your work notes to the issue. |
| Confidentiality | |
| Confidential | Option to enable confidentiality of the record. Only the assigned confidential users or confidential groups of users can access the record.<br><br>For more information on the confidential option, see Confidentiality flag for audit and compliance records. |
| Risk Event | |
| Risk event | The related risk event. |

3. Save the issue record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The tabs at the bottom of the screen enable you to perform various tasks for remediating the issue. You can add policy exceptions and create remediation tasks. Additionally, you can view other issues, indicator results, and task SLAs related to the issue.

**Note:** Starting with Version 12.0.1, the **Task SLA** tab creates and displays SLAs based on the **Due date**. Notifications are sent to the issue owner and issue manager when the issue **Due date** reaches 50%, then 75%, then when it breaches. If the **Assigned to** and **Due date** fields are not empty and the issue is not in the **New** state, an SLA is created for the issue.

If the due date for the SLA changes, a new SLA is created. The SLA is completed when the issue transitions to **Closed Complete** or **Closed Incomplete**. Also, the SLA is cancelled if the **Due date** or **Assigned to** fields are empty, or the state is New.

Also starting with Version 12.0.1, remediation tasks can be created with the Assigned to user and issue manager user roles, as well as any user with the GRC Business User role.

### Report issues from the Service Portal

When you identify any deficiencies in the controls or improvements that can be made in the organization policies, report an issue from the ServiceNow, Inc. Service Portal.

#### Before you begin

Role required: ServiceNow user

#### Procedure

1. In the Service Portal, click **Catalog** > **Browse by Categories**.
2. Click **Governance Risk and Compliance** and then click **Report Issue**.
3. On the form, fill in the following fields:

**Report Issue form**

| Field | Description |
|---|---|
| Enter a brief description of the issue | Brief description of the issue. |
| Enter a detailed description of the issue | Detailed description of the issue. |
| Enter possible suggestions to address the issue | Potential suggestions to address the issue. |
| Which entity is the issue related to? | Entity related to the issue. |
| Which control objective is the issue related to? | Control objective related to the issue.<br>**Note:**<br>This field appears only if Policy and Compliance Management is installed. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Which control is the issue related to? | Control inherited from item generation process. The control objective is read-only field. When you select the control, the control objective is auto-populated. |

4. Click **Submit**.
5. To view all the issues you have reported, navigate to **GRC > My Reported Issues**.

### Issue assignment using the Governance, Risk, and Compliance Predictive Intelligence plugin

Train a similarity solution model that uses machine learning so that the system can automatically suggest how to route issues to the correct assignee. Automatic routing suggestion reduces the time spent on deciding who should own the issue.

The Governance, Risk, and Compliance: Predictive Intelligence plugin utilizes Artificial Intelligence (AI) and Machine Learning (ML) to make GRC issue management smarter. On the GRC issue form, users are given suggestions for the assignment of issues to appropriate candidates. These suggestions are based on the platform similarity solution model.

Users must train the solution definition after they install the GRC: Predictive Intelligence plugin along with its dependencies. The Platform Machine Learning Administrator (ml_admin) can also customize the solution definition. This modification is based on the data in tables. Some of the critical fields, such as the filter condition **Assigned to [is] [not empty]**, must not be modified because modification may impact how the UI shows the prediction results.

### Train and use the similarity solution definition for issue assignment prediction

Train and use the machine learning solution by activating the Governance, Risk, and Compliance Predictive Intelligence plugin. The solution enables the system to automatically suggest correct assignees to route issues. These suggestions reduce the time spent on deciding who should own the issue.

#### Before you begin

Make sure that the following plugins are activated.

- The Policy and Compliance Management plugin
- The Risk Management plugin
- GRC Profiles plugin must be activated
- The Predictive Intelligence plugin

Modify the following  with the sn_grc.admin role.

- **Issue assignee suggestion based on** property (*`Similarity Analysis`*).
- **Machine Learning Solution for prediction of issue assignee** property (*`ml_sn_global_global_similarity_solution_definition_for_assigned_to_for_issue`*).

Role required: ml_admin

#### Procedure

1. Navigate to **Predictive Intelligence** > **Similarity** > **Solution Definitions**.
2. Click the **Similarity Solution Definition for Assigned To for Issue** solution.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Similarity Definition form

| Field | Value |
|---|---|
| Label | Unique name for the similarity solution. |
| Name | Name of the similarity solution. This field is automatically set to the system-assigned name that is the most similar to your value for the **Label** field. |
| Word Corpus | Existing word corpus that is relevant to your solution. For this use case, select the **Word Corpus for Issue Assignment** word corpus.<br><br>**Note:** For word corpora in similarity solutions, the number of records per table is limited to 300,000. |
| Table | Table that contains the records that you want to train against and to predict for. When you assign a table value, a link appears in the form. The link shows the number of records that match your current conditions.<br><br>For this use case, the field is automatically set to the Issue [sn_grc_issue] table. Do not modify this field for this solution definition. |
| Fields | Field types that are likely to help in identifying the owner. You can select the columns from the table in the **Table** field so that their data helps in predicting the issue more accurately. In this use case, the **Short description** and the **Description** fields are selected. These fields are the field types that contain the text of the issue records whose owner you're trying to identify.<br><br>**Note:** You can modify the fields selected here if there are other non-empty important fields on the issue record in your database, such that these fields can help in finding out similar issues for predicting the issue owners. |
| Test Table | Table that contains the record that you want to predict for. For this use case, the field is automatically set to the Issue [sn_grc_issue] table.<br><br>**Note:** The number of records which the Similarity window can retrieve is limited to 10. This field must not be modified for this solution definition. |
| Test Fields | Fields which are used as input during prediction. In this use case, select **Short description** and **Description**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Value |
| --- | --- |
| | **Note:** You can modify the fields selected here if there are other non-empty important fields on the issue record in your database, such that these fields can help in finding out similar issues for predicting the issue owners. |
| Filter | Filter that applies conditions to the field records that you're using as a base to retrieve your similarity results. For example in this use case, you can set an **Assigned to [is] [not empty]** condition because leaving the field empty will not provide a suggestion. |
| Processing Language | Dominant language of the dataset that you are training on the solution definition. If the dataset language is English, choose **English**.<br><br>By default, English processing is applied to all datasets. For example, if you select **Italian**, the system processes the data in both English and Italian.<br><br>**Note:** The term processing indicates some of the language-specific steps that are used as part of training a solution. These steps include tokenizing words, removing stop words, and stemming. |
| Stopwords | List of stopwords. When you select your processing language, the system automatically adds a Stopwords list that uses the same language. For example, if your processing language is English, the **Default English Stopwords** option appears. The Default English Stopwords list also appears in your selection. You can add your own custom list of stopwords. |
| Training Frequency | Frequency of training. The retraining option can range from once a day to every 30 days in 3 month increments up to 180 days. |
| Update Frequency | Frequency of how often you want to refresh the data that you use to retrieve your similarity results.<br><br>For example, new issues typically occur frequently throughout the day. If you have issue records that are open, you may want to select an update frequency of **Every 15 minutes**. This frequency can increase the likelihood that newly opened records are included in the refresh. |

3. Click the appropriate button for the solution definition.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| Save | Save your solution definition record so that you can return to it later. |
| Update and Retrain | Modify your solution definition and train it. |

## Use entity and risk dependencies using the GRC: Workbench

The GRC: Workbench utilizes CMDB information to show the upstream and downstream relationships across all applications. These relationships enable consistent risk mapping and modeling across the enterprise.

The GRC Manager [sn_grc.manager] uses the GRC Workbench to:

- Create entity classes.
- Define the upstream/downstream relationships between entity classes. These relationships make up the dependency model and ensure that risks are defined and evaluated consistently across the enterprise.
- Create entity types, create entities, and classify entities

**Note:** The GRC Manager cannot view the GRC: Workbench from **Risk** > **GRC Workbench**. The GRC Manager [sn_grc.manager] enters `/$grc_workbench.do` after their instance name in the url to access the GRC: Workbench.

The Risk Manager [sn_risk.manager] uses the GRC: Workbench to:

- Perform all the same tasks as the GRC Manager
- Create risk frameworks, risk statements, and risks
- Define risk relationships

## Model Setup tab

The Model Setup tab contains links to perform the following tasks.

| Link | Action |
| --- | --- |
| Dependency Model | Create entity classes and develop the organizational relationship model |
| Entity Types | Create and edit entity types |
| Dependency Map | Create and visualize entity relationships |

## Risk Dependencies tab

The Risk Dependencies tab contains links to perform the following tasks.

| Link | Action |
| --- | --- |
| Risk Frameworks | Create and edit risk frameworks |
| Risk Statements | Create and edit risk statements |
| Relationships | Create and visualize risk relationships |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Activate GRC: Workbench

The GRC: Workbench plugin is not activated by default, it is available as a separate subscription within the GRC Suite.

#### Before you begin
Role required: admin

#### About this task
To create entity classes, entity dependencies, and risk dependencies activate the GRC: Workbench, and the GRC: Risk Management plugin [com.sn_risk].

#### Procedure
1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the plugin using the filter criteria and search bar.

   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel.

3. Select **Install**, and then in the Activate Plugin dialog box, select **Activate**.

   **Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: `Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.`

Related topics

List of plugins

### Create entity class using the GRC: Workbench

GRC managers create entity classes representing the types of things that are part of the dependency model. Reports can be filtered to define relationships between the different enity classes. An entity class defines what a entity actually is.

#### Before you begin
Role required: sn_grc_manager

#### Procedure
1. Navigate to `https://myCompany.service-now.com/$grc_workbench.do`.
2. On the left, in the Entity classes section, click **Add Class**.
3. Enter an entity class name and click the plus (+) icon

   The newly created entity class is added to the list on the left.

#### What to do next
Create relationships between entity classes using the GRC: Workbench.

### Create relationships between entity classes using the GRC: Workbench

Managers create relationships between entity classes using the GRC: Workbench to build out the dependency map and better understand how entities relate to one another.

#### Before you begin
Role required: sn_grc.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create profile classes using the GRC: Workbench, before creating relationships between entity classes.

Entity classes can roll up to each other, leading to the development of the dependency model.

### Procedure

1. Navigate to `https://myCompany.service-now.com/$grc_workbench.do`.
2. Select the **Model Setup** tab at the top, and select the **Dependency Model** tab.
3. If needed, create entity classes.
4. Do one of the following actions.

| Option | Description |
|---|---|
| If there are no relationships between entity classes | Drag an entity class from the left to the center and drop it. |
| If there are relationships between entity classes | Drag additional entity classes from the list on the left and drop them on the top or bottom of any entity class in the tree.<br>**Note:** Dragging to the top of an entity class makes the target entity class roll up to the class that is dropped. Dragging to the bottom of an entity class makes the class that is being dropped roll up to the target class. |

**Note:** As long as you remain on the GRC: Workbench, click **Undo** after creating a relationship between entity classes to roll back the change. Leaving the GRC: Workbench causes the undo history to be lost.

### What to do next

After modeling out entities, define the risks in your organization:

- Generate a risk from a risk framework
- Generate a risk from a risk statement
- Associate a risk framework or risk statement with an entity type to generate risks

After generating risks, Relate risks to each other.

#### Associate a risk framework or risk statement with an entity type to generate risks

Risks are automatically generated when you make associations between risk frameworks or risk statements and entity types.

### Before you begin

Role required: sn_risk.admin and sn_risk.manager

### Procedure

1. Navigate to **Risk** > **Scoping** > **Entity types**.
2. Open the entity type record.
3. In the **Risk Framework** or **Risk Statement** related list, click **Edit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select the risk frameworks or risk statements to associate to the entity, and click **Save**.
   All risk frameworks or statements are associated to the entity type and a risk is created for every risk statement against every entity in the entity type.

### Visualize and edit entity dependencies using the GRC: Workbench

The GRC: Workbench gives GRC administrators a graphical interface to create entity dependencies. These relationships enable consistent entity and risk mapping and modeling across the enterprise.

#### Before you begin

Role required: sn_grc.manager

#### Procedure

1. Navigate to `https://myCompany.service-now.com/$grc_workbench.do`.
2. Select the **Model Setup** tab at the top, then select the **Dependency** tab below it.
3. Search for and select an entity from the list on the left.
   Entities are organized hierarchically by entity class, then by entity types.
4. After selecting an entity from the left, the entity is displayed in the center with its direct upstream and downstream dependencies.
   On the right, eligible entities that can be added as upstream or downstream dependencies are listed.
5. Perform one of the following actions.

| Option | Description |
|---|---|
| To add an upstream entity dependency | Drag an eligible upstream entity from the list of eligible entities on the right and drop it on the top half of the entity in the center of the page. |
| To add a downstream entity dependency | Drag an eligible downstream entity from the list of eligible entities on the right and drop it on the bottom half of the entity in the center of the page. |

   The entities are removed from the right menu when moved to the center of the page.

### Delete entity dependencies using the GRC: Workbench

When deleting entity dependencies, only the relationship between the entities is deleted. The entities themselves remain unmodified.

#### Before you begin

Role required: admin

#### Procedure

1. Navigate to `https://myCompany.service-now.com/$grc_workbench.do`.
2. Select the **Model Setup** tab at the top, then select the **Dependency Map** tab below it.
3. Search for and select the desired entity from the list on the left.
   After selecting an entity from the left, the entity is displayed in the center with its direct upstream and downstream dependencies.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. In the center tree, point to the upstream or downstream risk that should be disassociated from the selected center risk.
   As you point to the risk, a delete icon appears, click the delete icon.
5. Click **Delete** in the confirmation dialog to confirm the deletion of the relationship.

> **Note:** Only the relationship between the entities is deleted. The entities themselves remain unmodified.

### Delete an entity class using the GRC: Workbench

Deleting an entioty class, deletes all relationships below it.

#### Before you begin
Role required: admin

#### Procedure
1. Navigate to `https://myCompany.service-now.com/$grc_workbench.do`.
2. Select the **Model Setup** tab at the top, and select the **Dependency Model** tab.
3. Select the desired entity class from the list on the left.
   After selecting an entity from the left, the entity is displayed in the center with its direct upstream and downstream dependencies.
4. Click the delete icon to the right of the entity class name.
5. In the deletion confirmation pop-up, click **Delete**.
   Deleting the entity class deletes all relationships below it.

### Create a risk using the GRC: Workbench

Risk managers can create risks directly from the GRC: Workbench.

#### Before you begin
Role required: sn._risk.admin or sn.risk.manager

#### Procedure
1. Navigate to `https://myCompany.service-now.com/$grc_workbench.do`.
2. Select the **Risk Dependencies** tab at the top, then select the **Relationships** tab below it.
3. On the left, in the Risks section, click **Create Risk**.
4. On the form, fill in the fields.

**Risk form**

| Field | Description |
|---|---|
| Name | Name for the risk. Field is auto-populated if the risk is generated from a risk statement, but can be changed without affecting the relationship between the risk and risk statement. |
| Number | Unique identification number. This field is automatically populated. |
| State | Risk state. Possible choices are: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ **Draft** In this state, all risk users can modify the risk. Only available when creating a one-off control. One-off controls are possible but not recommended.<br>◦ **Attest** When the risk is created from a risk statement, controls are in this state.<br>**Note:** When a risk is set back to draft, the assessment is canceled.<br>◦ **Review** Risks are automatically moved to review from the assessment phase.<br>◦ **Monitor** In this state, all risk managers can move the risk from review to monitor.<br>◦ **Retired** Risk managers or administrators can move a risk from Monitor to Retired. Indicators do not run when the risk is in this state.<br>**Note:** When a risk is retired, any assessment associated with it is canceled. |
| Owning group | Owning group for the risk. |
| Category | Category of risk which applies to the profile.<br>◦ Legal<br>◦ Financial<br>◦ Operational<br>◦ Reputational<br>◦ Legal/Regulatory<br>◦ Credit<br>◦ Market<br>◦ IT<br>Field is auto-populated if risk is generated from a risk statement. |
| Owner | Owner for the risk.<br>**Note:** The owner is always added as a respondent. |
| Statement | Statement this risk is associated with. |
| Entity | Entity related to the risk.<br>**Note:** Only active entities are shown. |
| Description | Description of the risk and how it is a threat to the organization. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Additional Information | More details that help others understand the risk record. |

5. Click the **Assessment** tab.
6. On the form, fill in the fields.

**Risk Scoring form**

| Field | Description |
|---|---|
| Assessment | Assessment to attach to this risk. |
| Assessment respondents | Users assigned to the assessment of this risk.<br>**Note:** Only a user with the sn_grc.user role can be added as a respondent. |

When both the **Assessment** and **Assessment respondents** fields are set, assessments are created when you click **Assess**.

7. Click the **Scoring** tab.
8. On the form, fill in the fields.

**Risk Scoring form**

| Field | Description |
|---|---|
| Inherent SLE | Monetary value of a risk if it occurs before any mitigation strategies are in place. |
| Residual SLE | Monetary value of a risk if it occurs after all mitigation strategies are in place. |
| Inherent ARO | Probability that a risk occurs in any given year before any mitigation strategies are in place. |
| Residual ARO | Probability that a risk will occur in any given year after all mitigation strategies are in place. |
| Inherent ALE | Annualized loss expectancy `ALE = SLE x ARO` before any mitigation strategies are in place. |
| Residual ALE | Annualized loss expectancy `ALE = SLE x ARO` after all mitigation strategies are in place. |
| Inherent score | The score of the risk before any mitigation strategies are in place. |
| Residual score | The score of the risk after all mitigation strategies are in place. |
| Calculated ALE | Annualized loss expectancy based off all calculations. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Calculated score | The corresponding score for the calculated ALE. |

9. Click the **Response** tab.
10. On the form, fill in the fields.

**Risk Response form**

| Field | Description |
|---|---|
| Response | ◦ Accept<br>◦ Avoid<br>◦ Mitigate<br>◦ Transfer |
| Justification | Enter a reasonable justification for the selected response |

11. Click the **Monitoring** tab.

**Risk Monitoring form**

| Field | Description |
|---|---|
| Control compliance | Percentage of compliant controls |
| Control non-compliance | Percentage of non-compliant controls |
| Control failure factor | Sum of failed controls weighting divided by total controls weighting |
| Indicator failure factor | Uses the last result of each associated indicator. Number of last results failed divided by total number of indicators associated. |
| Calculated risk factor | This value is calculated from `(Indicator failure factor + Control failure factor) / 2`. |

12. Click the **Activity Journal** tab.
13. Enter additional comments, as necessary.
14. Click **Submit**.
    The risk is created and centered in the middle of the page. Also, the risk is selected on the right.

### Visualize and edit risk dependencies using the GRC: Workbench

The GRC: Workbench gives GRC administrators a graphical interface to create risk dependencies. These relationships enable consistent entity and risk mapping and modeling across the enterprise.

#### Before you begin

Role required: sn_risk.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to `https://myCompany.service-now.com/$grc_workbench.do`.
2. Select the **Risk Dependencies** tab at the top, then select the **Relationships** tab below it.
3. Search for and select a risk from the list on the left.
   Risks are organized hierarchically by entity class, then by entity.
4. After selecting a risk from the left, the risk is displayed in the center with its direct upstream and downstream dependencies.
   On the right, eligible risks that can be added as upstream or downstream dependencies are listed.
5. Perform one of the following actions.

| Option | Description |
|---|---|
| To add an upstream risk dependency | Drag an eligible upstream risk from the list of eligible risks on the right and drop it on the top half of the risk in the center of the page. |
| To add a downstream risk dependency | Drag an eligible downstream risk from the list of eligible risks on the right and drop it on the bottom half of the risk in the center of the page. |

#### Delete risk dependencies using the GRC: Workbench

When deleting risk dependencies, only the relationship between the risks is deleted. The risks themselves remain unmodified.

### Before you begin

Role required: sn_risk.manager

### Procedure

1. Navigate to `https://myCompany.service-now.com/$grc_workbench.do`.
2. Select the **Risk Dependencies** tab at the top, then select the **Relationships** tab below it.
3. Search for and select a risk from the list on the left.
   Risks are organized hierarchically by entity class, then by entity.
4. In the center tree, point to the upstream or downstream risk that should be disassociated from the selected center risk.
   As you point to the risk, a delete icon appears, click the delete icon.
5. Click **Delete** in the confirmation dialog to confirm the deletion of the relationship.

> **Note:** Only the relationship between the risks is deleted. The risks themselves remain unmodified.

## Monitor risks using GRC Performance Analytics Indicators

You can link Risk Management risk statement and risks to Performance Analytics indicators, breakdowns and thresholds. You can associate Performance Analytics indicators with risk statements, and risks to view scorecards and trends and analyze current conditions and trends.

The risks and controls associated with a PA indicator or PA indicator/breakdown/element automatically monitor any PA threshold with the same PA indicator or PA indicator,

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

breakdown, or element relationship. Any PA threshold breach is reported at the risk or control and Performance Analytics indicators relationship level within a breach counter.

## PA threshold breach impact

When a risk or control and Performance Analytics indicators relationship breach counter is different than zero (for example, a PA threshold with the same PA indicator or PA indicator, breakdown, or element relationship has breached), and if no opened issue exists, then an issue is created which is associated to the risk or control. Also for risks, the **Indicator failure factor** represents the number of risk and Performance Analytics indicators relationships with a breach counter different than zero.

## Reset all PA Indicator breach counters

Reset breach counters associated to a risk or control by clicking **Reset all PA Indicator breach counters** or opening the specific relationship and clicking **Reset Breach Counter**.

## GRC PA indicator breach reports

There are two reports for the reporting of breaches:

- Risk PA Indicator Breaches
- Control PA Indicator Breaches

### Activate GRC: Performance Analytics Integration

The GRC: Performance Analytics Integration plugin provides an integration between Performance Analytics and the Risk Management and Policy and Compliance Management applications. This plugin provides more insight into organizational risk and compliance performance.

**Before you begin**
Role required: admin

**About this task**
This plugin includes demo data and activates related plugins if they are not already active.

**Procedure**

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.
2. Find the plugin using the filter criteria and search bar.

   You can search for the plugin by its name or ID. If you cannot find a plugin, you might have to request it from ServiceNow personnel.

3. Select **Install**, and then in the Activate Plugin dialog box, select **Activate**.

   **Note:** When domain separation and delegated admin are enabled in an instance, the administrative user must be in the **global** domain. Otherwise, the following error appears: `Application installation is unavailable because another operation is running: Plugin Activation for <plugin name>.`

**What to do next**
After activating the GRC: Performance Analytics Integration plugin on an instance with customized related lists on content (risk or control objective) or items (risk or control), you may have to manually add the PA Indicator to content relationships and/or the PA indicator to item relationships.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

List of plugins

### Associate a PA indicator with a risk statement or control objective

You can associate Performance Analytics indicators with risk statements and policy statements to analyze trends related to the risk or policy.

#### Before you begin

Role required: sn_risk.manager or sn_compliance.manager

#### Procedure

1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Policies and Procedures** > **Control objectives**.
   - **All** > **Risk** > **Risk Library** > **Risk Statements**.
2. Open a risk statement or control objective.
3. In the **PA Indicators** related list, click **New**.
4. On the form, fill in the fields.

**PA Indicators form**

| Field | Description |
|---|---|
| PA Indicator | The performance analytics indicator to associate the Risk Statement or control objective with. |

5. Click **Submit**.
   On the risk statement or control objective form, in the **PA Indicators** related list, you see the associated indicator. You can optionally click **View Indicator** on the desired indicator to see the Performance Analytics scorecard of the indicator. The PA Indicator associations are carried over to all risks or controls associated to the original risk statement or control objective. Also, if the indicator has a breakdown that matches the risk or entity of the control (for example a Business Service breakdown), the **Breakdown** and **Element** fields for the relationship are automatically filled in.

### Associate a PA indicator with risks and controls

You can associate Performance Analytics indicators with risks and controls to analyze trends related to the entity that risk or control belongs to.

#### Before you begin

Role required: sn_risk.manager or sn_compliance.manager

#### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Controls** > **All Controls**.
   - **Risk** > **Risk Register** > **All Risks**.
2. Open a risk or control.
3. In the **PA Indicators** related list, click **New**.
4. On the form, fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**PA Indicators form**

| Field | Description |
|---|---|
| PA Indicator | Performance analytics indicator to associate the Risk or Control with. |
| Breakdown | Break down to view a specific trend based on the breakdown element. |
| Element | Break down element to view a particular trend and scorecard.<br><br>**Note:** This field depends on the **Breakdown** field being populated. When visible, it is mandatory. |

5. Click **Submit**.
   On the Risk or Control form, in the **PA Indicators** related list, you see the associated indicator. You can optionally click **View Indicator** on the desired indicator to see the Performance Analytics scorecard of the indicator.

### Update associated GRC indicators for a set of items

You can update all the items belonging to a GRC content record so each item is individually related to the PA indicator.

#### Before you begin
Role required: sn_risk.manager or sn_compliance.manager

#### Procedure

1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Policies and Procedures** > **Control Objectives**.
   - **All** > **Risk** > **Risk Library** > **Risk Statements**.
2. Open a Risk Statement or Control Objective that has an associated Performance Analytics Indicator.
3. Click the **Update PA Relationships** related link.
   All the risks or controls related to the risk statement or policy statement are automatically associated with all the risk statement or policy indicators of the statement. Also, if the indicator has a breakdown that matches the risk or entity of the control (for example a Business Service breakdown), the **Breakdown** and **Element** fields for the relationship are automatically filled in.

## Create a GRC indicator template

Compliance or risk managers create indicator templates from which many indicators can be created.

#### Before you begin
Role required:

- sn_compliance.admin or sn_compliance.manager
- sn_risk.admin or sn_risk.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_audit.admin or sn_audit.manager
- sn_grc.user

### Procedure

1. Navigate to one of the following locations:
   - **All** > **Policy and Compliance** > **Indicators** > **Indicator Templates**.
   - **All** > **Risk** > **Indicators** > **Indicator Templates**.
2. Click **New**.
3. On the form, fill in the fields.

**Indicator template form**

| Field | Description |
|---|---|
| Name | Name of the indicator. |
| Description | Description of the indicator. |
| Category | Category for which you are creating an indicator template. For example, select **Risk Indicator Template** to create a risk indicator template. |
| Active | Option that determines whether the indicator template is active. |
| Method | |
| Type | Method used to determine the type of indicator template. The choices are as follows:<br>◦ **Manual**: Manual indicators are used for data that cannot be retrieved from a ServiceNow instance because it comes from an external system, such as customer data from a third-party sales system.<br>◦ **Basic**: Basic indicators are automated indicators based on an indicator source. The indicator source specifies a table and a frequency at which the scores from this table are saved.<br>◦ **Script**: Scripted indicators use a custom script to collect the data. |
| Result if the value meets or exceeds the target value | Result configuration field. The choices are as follows:<br>◦ **Passed**<br>◦ **Failed**<br>For example, assume you enter `100` in this field. If the indicator result output is more than 100, then the indicator status will pass |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | or fail based on the value configured in this field. |
| Target Type | Type of the target value. The choices are as follows:<br>◦ **None**: Use this option if you do not want to set up any target or threshold for the indicator.<br>◦ **Percentage**: Use this option to determine the indicator result by a percentage value.<br>◦ **Count**: Use this option to determine the indicator result by a count value or total number. |
| Target | Value to determine if the indicator will pass or fail. |
| Instructions | Additional instructions for the template. |
| Value mandatory | Option to decide if a value must be compulsory in the indicator task for a manual indicator.<br>**Note:** This option appears only if **Manual** is selected from the **Type** field. This option is automatically selected if **Count** or the **Percentage** is selected from the **Target type** field. |
| Supporting Data | |
| **Note:** Starting with version 10.1, the actual historical data for the supporting data records from the indicator results or indicator tasks is displayed. Earlier, only the real-time state of the records collected could be viewed. | |
| Collect supporting data | Option to enable collecting supporting data or evidence every time the indicator runs. |
| Table | Table used for collecting supporting data. |
| Supporting data fields | Fields of the source table to be used for collecting the supporting data. |
| Sample collection type | Type of supporting data collection, such as count or percentage. |
| Sample size | Minimum number of records that must be used for collecting supporting data.<br>For example, a basic indicator could query a large table, returning thousands of records with each indicator execution. You do not need to save all of them; just a sample of those records. If you enter a |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | sample size of 100, only 100 records are saved, even though the query returned thousands. |
| Basic Criteria | |
| Criteria | Criteria to filter the data from the source table. |
| Use reference field | Option to enable the use of the **Reference field**. |
| Reference field | Connection between the supporting data table and the **Applies to record** field of the entity. |
| Additional Criteria | |
| To create indicators with targets, use the advanced filter criteria. This section appears only when you select **Basic** from the **Type** field. This section is used to provide more filter criteria. | |
| Additional criteria | More criteria to filter the data to calculate the target value. This section only appears when **Percentage** is selected from the **Target type** field. |
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| First run date | First collection time for indicator results. This field is automatically set based on when an indicator or an indicator template runs for the first time. The value in this field cannot be modified. |
| Next run date | Next run time to collect indicator results of all downstream indicators for this indicator template. |
| Due date duration (days) | Due date duration in days between the creation and due date of the indicator task and generation of its results.<br><br>The due date duration added to the creation date reflects as the **Due date** of the indicator task.<br><br>This field appears only when **Manual** is selected from the **Type** field.<br><br>For more information, see Performance enhancements for Indicator nightly job. |

4. When you have completed these entries, you can also view information on the following related lists:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Control Objectives/Risk Statements
- Content References

**Note:** The **Control Objectives/Risk Statements** tab enables you to reuse the same template for multiple control objectives or risk statements, or both of them.

5. Select **Submit**.

## Create a risk indicator

Create a risk indicator to identify the possibility of a future adverse impact on your organization. Indicators are an early warning system, and they enable you to take preventative action on the risks.

### Before you begin

Role required: sn_risk.manager or sn_risk.admin

### About this task

Generally, indicators are automatically created using the normal process of indicator templates. You can also manually create new indicators. You can also create an indicator by using an indicator template. When you relate an indicator template to a risk statement, the risk indicators are automatically generated.

### Procedure

1. Navigate to **All** > **Risk** > **Indicators** > **Indicators**.
2. Click **New**.
3. On the form, fill in the fields.

**Indicator form**

| Field | Description |
|---|---|
| Category | Category of the indicator. For example, select **Risk Indicator** to create a risk indicator. |
| Inherit from template | Option to create the indicator from an existing template. |
| Template | Template used to create the indicator. This field appears only if the **Inherit from template** option is selected. |
| Override template | Option to override the template's properties such as the name of the indicator. |
| Name | Name of the indicator. If you select a template in the **Template** field, then this field is automatically set to the template name. |
| Description | Brief description of the indicator. This field is automatically set if you select a template in the **Template** field. |
| Entity | Entity used to filter risks. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Applies to record | Record that the entity applies to. |
| Risk | Filtered risk that is related to the indicator.<br><br>**Note:** If you have selected an indicator template, then the risk is also filtered based on the template. |
| Owning group | Group that owns the indicator. |
| Owner | Owner of the indicator. This field is automatically set to the owner's name based on the risk. |
| Method | |
| Type | Method used to determine the type of indicator. The choices are as follows:<br>◦ **Manual**: Manual indicators are used for data that cannot be retrieved from a ServiceNow instance because it comes from an external system, such as customer data from a third-party sales system.<br>◦ **Basic**: Basic indicators are automated indicators based on an indicator source. The indicator source specifies a table and a frequency at which the scores from this table are saved.<br>◦ **Script**: Scripted indicators use a custom script to collect the data. |
| Target type | Type of the target value. The choices are as follows:<br>◦ **None**: Use this option if you do not want to set up any target or threshold for the indicator.<br>◦ **Percentage**: Use this option to determine the indicator result by a percentage value.<br>◦ **Count**: Use this option to determine the indicator result by a count value or total number. |
| Value mandatory | Option to decide if a value must be compulsory in the indicator task for a manual indicator.<br><br>**Note:** This option appears only if **Manual** is selected from the **Type** field. This option is automatically selected when **Count** or **Percentage** is selected from the **Target type** field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Target | Value to determine if the indicator will pass or fail. |
| Result based on target value | Result configuration field. The choices are as follows:<br>◦ **Passed**<br>◦ **Failed**<br>For example, assume you enter `100` in this field. If the indicator result output is more than 100, then the indicator status will pass or fail based on the value configured in this field. |
| Instructions for collecting data | More instructions on how to collect data. |
| Supporting Data | |
| **Note:** Starting with version 10.1, the system displays the actual historical data for the supporting data records from the indicator results or indicator tasks. | |
| Collect supporting data | Option to enable collecting supporting data or evidence every time the indicator runs. |
| Source table | Table used for collecting supporting data. |
| Supporting data fields | Fields of the source table that are used for collecting the supporting data. |
| Sample size | Minimum number of records that must be used for collecting supporting data. |
| Basic Criteria | |
| To filter the data on the source table, use the basic criteria. This section appears only when **Manual** or **Basic** is selected from the **Type** field. | |
| Criteria | Criteria to filter the data from the source table. |
| Use reference field | Option to enable the use of the **Reference field**. |
| Reference field | Connection between the supporting data table and the **Applies to record** field of the entity. |
| Additional Criteria | |
| To create indicators with targets, use the advanced filter criteria. This section appears only when you select **Basic** from the **Type** field. This section is used to provide more filter criteria. | |
| Additional criteria | More criteria to filter the data to calculate the target value. This section only appears when **Percentage** is selected from the **Target type** field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| Next run time | Next collection time for indicator results. This field is automatically set based on the value in the **Collection frequency** field. |
| Results | |
| Status | Status of the indicator to show whether the indicator passed or failed. |
| Previous status | Previous status of the indicator to show whether the indicator passed or failed. |

4. Click **Submit**.

**Result**
The risk indicator is created and is ready to be executed.

## View the Risk Overview

The Risk Overview is contained in the Risk Management application and provides an executive view, allowing risk managers to quickly identify areas of concern by pinpointing entities with known high risk.

The Risk Overview contains the following reports in the base system.

### Risk Overview

| Name | Visual | Description |
|---|---|---|
| Inherent Risk | | |
| Residual Risk | | |
| Inherent Annual Loss Exposures | | |
| Residual Annual Loss Exposures | | |
| Risk Issues by Framework (Opened Date) | | |
| Risks by Response | | |
| Risk Expectations | | |
| Profile | Drop down list | Select one or many profiles to view and compare their risks. |
| GRC - Risk States | Check boxes | Select one or many risk states to view and compare. |
| Risks by Category | | |
| Very High Risk | Single Score | Displays the number of very high risks. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk Overview (continued)**

| Name | Visual | Description |
|---|---|---|
| High Risk | Single Score | Displays the number of high risks. |
| Moderate Risk | Single Score | Displays the number of moderate risks. |
| Low Risk | Single Score | Displays the number of low risks. |
| Very Low Risk | Single Score | Displays the number of very low risks. |
| Inherent Risk Heatmap | | |
| Residual Risk Heatmap | | |

## Using the Risk Workspace

Starting with Version 13.0.5, a new workspace has been introduced for the Risk Management application. The new workspace provides you with an improved User Experience (UX) and a simplified user journey.

### Create a risk framework in the Risk Workspace

Create risk frameworks to group risk statements into manageable categories and generate risks. After the risks are generated, you can identify methods to mitigate them.

**Before you begin**
Role required: sn_risk.manager

**Procedure**

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Library** > **Risk frameworks**.
2. Click **New**.
3. On the form, fill in the fields.

**Risk Framework form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Active | Option to indicate whether the risk framework is active.<br>**Note:** If a risk framework is made inactive or retired, all the associate risk statements and risk records are also deactivated. |
| Name | Name of the risk framework. |
| Description | Description of the risk framework. |
| Additional information | Additional information for this risk framework. |

4. Click **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. To add entities from entity types, click the Entity types related list.
   a. Click **Add**.
   b. Select the entity types.
   c. Click **Add**.
6. To add risk statements, click the Risk Statements related list and do one of the following.

| Choice | Steps |
|---|---|
| To add an existing risk statement | a. Click **Add**<br>b. Select the risk statement.<br>c. Click **Add**. |
| To create a risk statement | a. Click **New**.<br>b. Select the risk statement and fill in the form.<br>For more information, see Create a risk statement in the Risk Workspace.<br>c. Click **Add**. |

### Result
The new risk framework is created.

## Create a risk statement in the Risk Workspace

Create risk statements to group risks into manageable categories.

### Before you begin
Role required: sn_risk.admin

### About this task
When you create a risk statement, you can associate entity types or add additional entities to generate risks.

**Note:** When any of the following risk statement fields changes: Name, Description, Reference, Category, Type, Classification, and Attestation, all the associated controls and risks are updated, and their state is set back to Draft. All the associated risk assessments also get canceled.

### Procedure
1. Navigate to **All** > **Risk Workspace** > **Library** > **Risk statements**.
2. Click **New**.
3. On the form, fill in the fields.

#### Risk Statement form

| Field | Description |
|---|---|
| Name | Name of the risk statement. |
| Description | Description of the risk statement. |
| Parent | Parent risk statement. You can define the hierarchy using this field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Framework | Framework this risk statement is associated with.<br><br>**Note:** This field only appears if the *Migrate to Advanced Risk Assessment* property is enabled. For more information, see Risk score rollup in Advanced Risk Assessment |
| Category | Category of the risk statement. The choices are as follows:<br>◦ Legal<br>◦ Financial<br>◦ Operational<br>◦ Reputational<br>◦ Legal/Regulatory<br>◦ Credit<br>◦ Market<br>◦ IT<br>◦ Project |
| Level | Level at which the risk statement is created. For example, if the risk statement has a parent and a grandparent, then the level of this new risk statement will be 3. |
| Assessment | Risk assessment template to be assigned to this risk statement. An assessment template is a questionnaire that is used for assessing a risk.<br><br>**Note:** This field appears when you use classic risk with enabling the advanced risk property. |
| Issue group rule | Issue group rule assigned to this risk statement for reporting. The purpose of the issue group rule is to group similar issues together into a parent issue based on conditions defined in the rule. This feature enables you to work on the similar issues at once and close out the parent issue once resolved, which will close out all the child issues. |
| Additional information | Additional information for this risk statement. |

4. To fill in the fields for the risk appetite section, see Define the risk appetite for a risk statement.
5. If you're using classic risk, in the Default Scores section, fill in the fields.

| Field | Description |
|---|---|
| Inherent SLE | Single-loss expectancy (SLE) is the monetary value expected from the occurrence of a risk on an asset if there are no controls to check the event. |
| Residual SLE | Monetary value expected from the occurrence of a risk on an asset if there are controls to check the event. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Inherent ARO | Annualized rate of occurrence (ARO) is an estimated frequency of the threat occurring in one year. ARO is used to calculate annualized loss expectancy (ALE). The value in this field indicates the likelihood of the event occurring if there are no controls to check the event. |
| Residual ARO | The value in this field indicates the likelihood of the event occurring if there are controls to check the event. |

6. If you're using classic risk with the advanced risk plugin activated, in the **Risk Rollup and Tolerance** section, fill in the fields.

| Field | Description |
| --- | --- |
| Expected ALE | ALE refers to the product of the ARO and the SLE. Expected ALE is the expected value of the ALE for the risk statement. Enter currency and amount for the expected ALE.<br><br>**Note:** This value must be less than or equal to the **Maximum acceptable ALE**. |
| Sum of calculated ALE | This calculation is based on the sum of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Maximum calculated ALE | This calculation is based on the maximum of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Maximum acceptable ALE | Threshold value for the ALE for the risk statement.<br><br>**Note:** This value must be greater than or equal to the **Expected ALE**. This value has an impact on the **Tolerance status** field. |
| Average calculated ALE | This calculation is based on the average of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Minimum calculated ALE | This calculation is based on the minimum of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Tolerance Status | Overall risk status. This field appears when the other ALE fields are populated. |
| Calculated Score | The corresponding score for the calculated ALE:<br>◦ Low<br>◦ Med<br>◦ High |

7. In the Basel Categorization section, select the Basel Categories Hierarchy.
   The Basel categories are as follows:
   - Internal Fraud: misappropriation of assets, tax evasion, intentional mismarking of positions, bribery.
   - External Fraud: theft of information, hacking damage, third-party theft, and forgery.
   - Employment Practices and Workplace Safety: discrimination, workers' compensation, employee health, and safety.
   - Clients, Products, and Business Practice: market manipulation, antitrust, improper trade, product defects, breaches, account churning.
   - Damage to Physical Assets: natural disasters, terrorism, vandalism.
   - Business Disruption and Systems Failures: utility disruptions, software failures, hardware failures.
   - Execution, Delivery, and Process Management: data entry errors, accounting errors, failed required reporting, negligent loss of client assets.
8. Click **Save**.
9. To add entity types, click the Entity types related list.
   a. Click **Add**.
   b. Select the entity types to add.
   c. Click **Add**.
10. To add additional entities, click the **Additional entities** related list.
    a. Click **Add**.
    b. Select the entities to add.
    c. Click **Add**.
11. Click **Save**.

### Result
The risk statement is created.

### What to do next
You can continue to add control objectives, indicator templates, and information objects to the risk statement. You can also now assess the risks that are generated in the Risks tab. You can also view the hierarchy of the risks statement on the risk statement side bar. To view the complete risk profile at a glance, click the **Overview** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Associate a risk statement with a control objective in the Risk Workspace

Associate risk statements to control objectives in the Risk Workspace. This association helps you to manage your risks by ensuring that the risks have mitigating controls.

### Before you begin

Role required: sn_risk.manager or sn_compliance.manager

### About this task

When a control objective and risk statement are associated and the control entity matches the risk entity, the risk-control association is created. This association helps in mitigating the risks and threats.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace**.
2. In the Risk Workspace, select the list icon.
3. Navigate to **Library** > **Control objectives**.
4. Select and open the required control objective.
5. Select the Risk statements related list.
   a. Select **Add**.
   b. Select the risk statements that you want to add.
   c. Select **Add**.
   d. Select **Save**.

### Result

The risks associated with the risk statement automatically inherit the controls associated with the control objectives with matching entities.

## Common controls in Risk Management

By linking the risks to a common control in the Risk Management application, you can reduce the time and effort that is needed to manage and apply these centralized controls to your reliant entities. For example, a fire sprinkler system can be a common control for multiple business units (BUs), such as finance, security, and human resources (HR).

## Overview of common controls

Every organization has multiple (BUs) and shared functions, such as information technology (IT), HR, and finance. These shared functions define the policies and controls that the BUs can use to meet the regulatory requirements or to manage the risks in their BUs. Multiple BUs can use common controls that are owned and managed by a different department or team. This process enables an organization to maintain centralized control over certain processes while each BU can take advantage of these common controls. For more information on common controls, see Common Controls.

To mitigate the risks in the reliant entities, a risk owner can link their risks to the common controls. By linking the risk, a risk owner can reduce the effort that is required to attest and test these common controls for the reliant entities.

## Benefits of common controls

A common control has the following benefits:

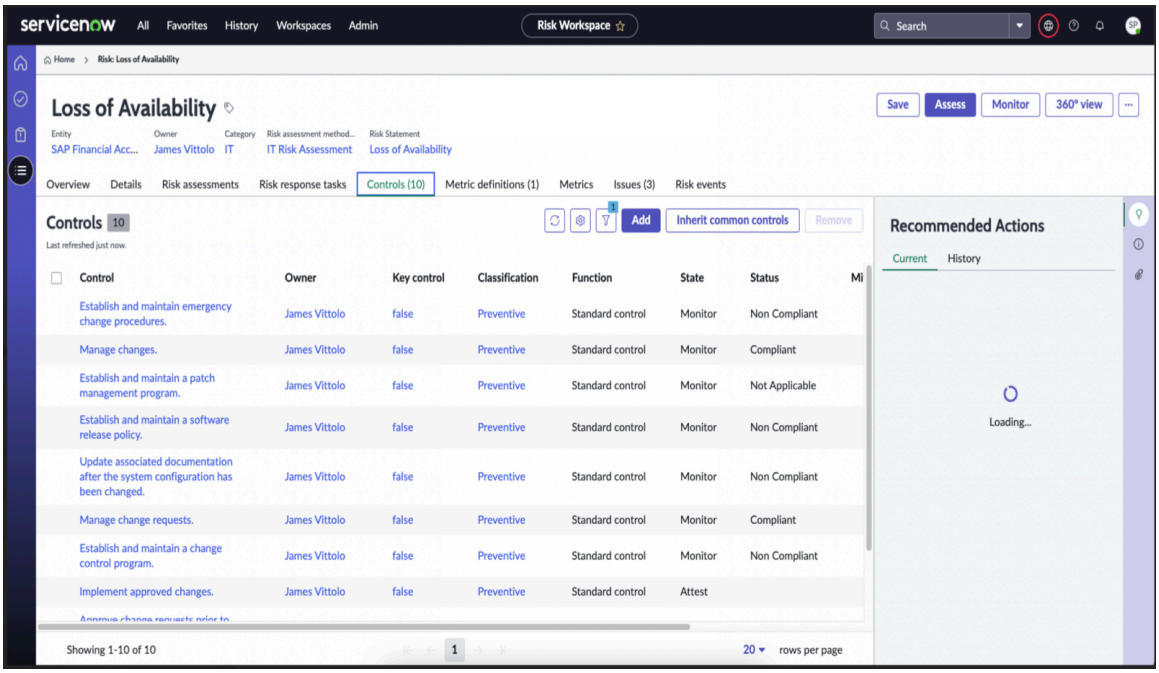
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- You spend less time and effort to manage a common control because you can test and apply a common control to all your reliant entities.
- You only need to manage the active controls, so the overall reporting of the controls is improved.

## Common controls in a risk

If a control objective and risk statement are associated and the reliant entity of the control matches the risk entity, the risk-control association is established automatically. You can also inherit common controls to a risk when the risk entity is marked as a reliant entity in a common control. Any changes to the risk statement and the control's objective relationship can impact the risk-control association as well. The following example shows the inherit common controls option on the risk form:

### Inherit common controls



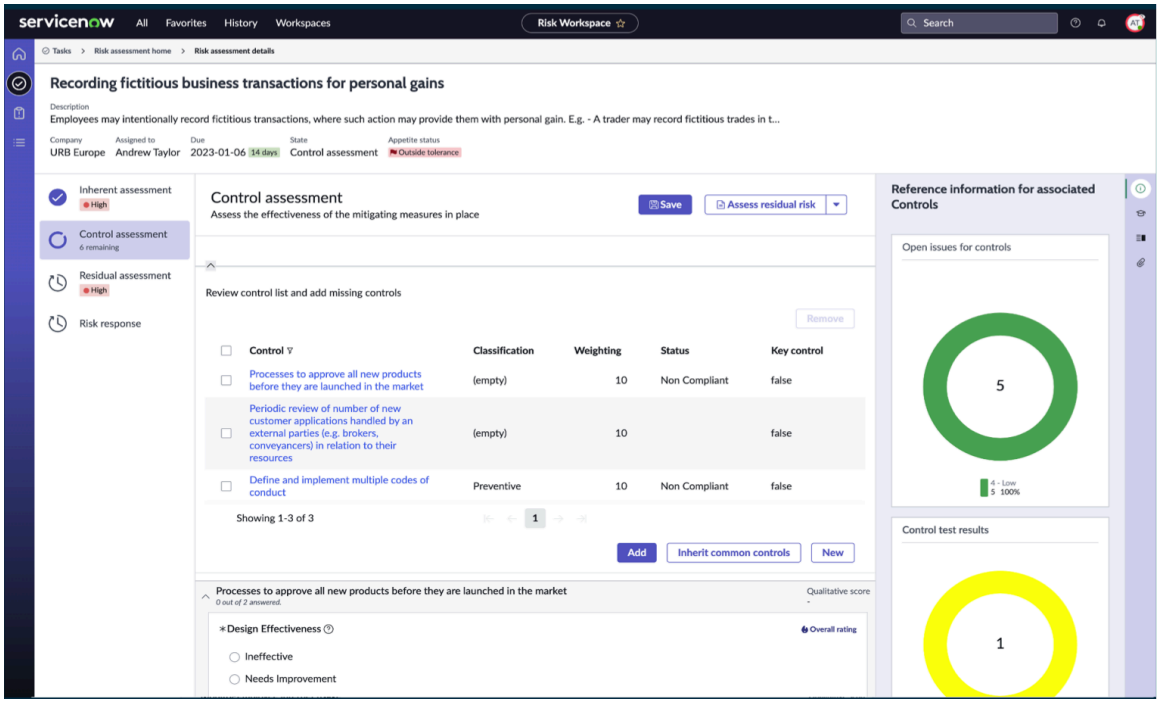

**Note:** Only active relationships between risks and controls are maintained and any historic relationships are automatically deleted.

## Common controls in a risk assessment

You can inherit common controls in the risk assessment when the entity is marked as a reliant entity in the common control. The following example shows the inherit common controls option on the risk assessment form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

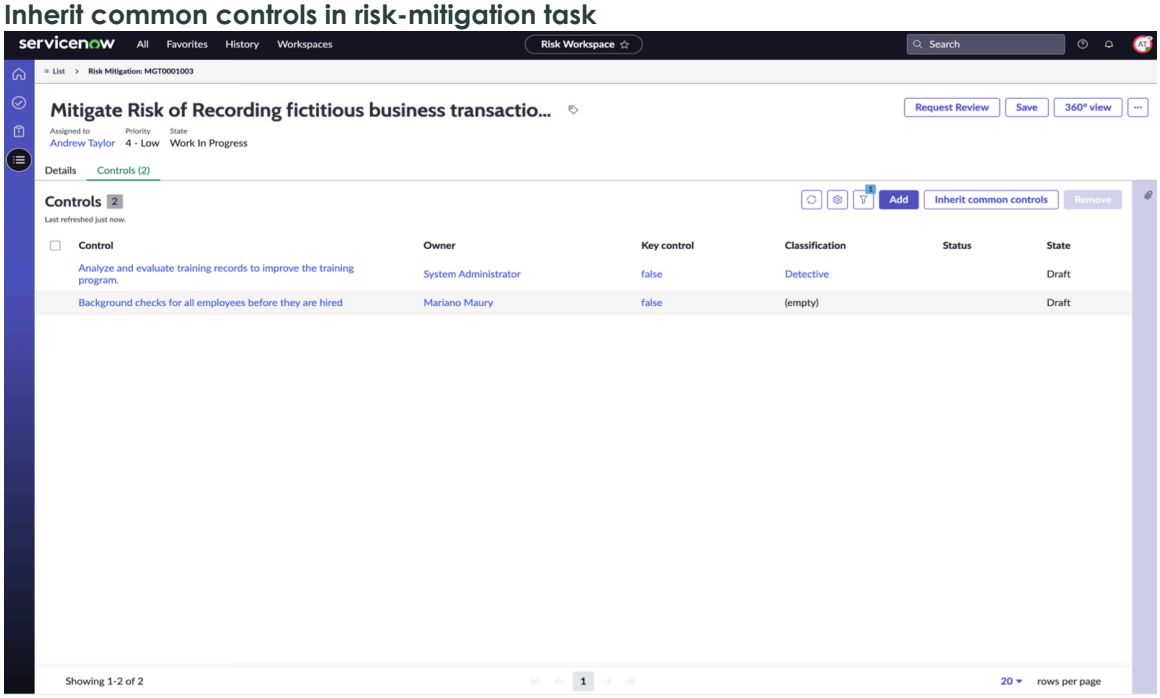
### Inherit common controls in risk assessment




## Common controls in a risk-mitigation task

You can inherit the common controls to a risk-mitigating task when the entity is marked as a reliant entity in the common control. You can inherit the common controls to a risk-mitigating task when it is in the Draft or Work In Progress state. The following example shows the inherit common controls option on the risk-mitigation task form.

### Inherit common controls in risk-mitigation task



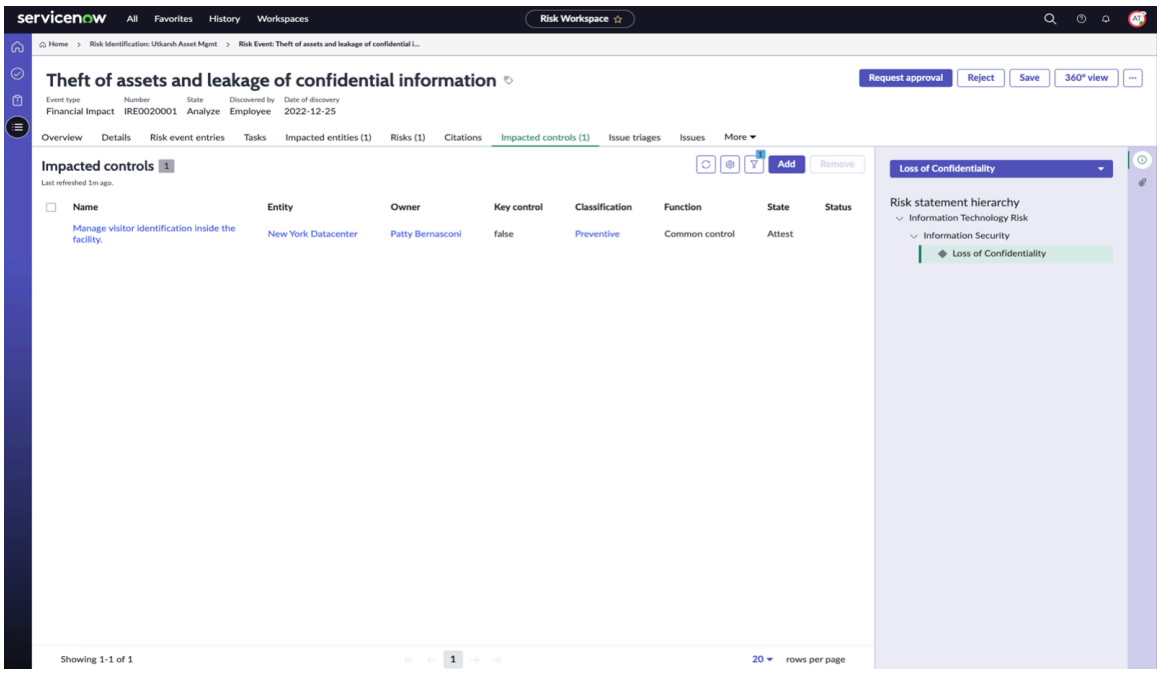

## Common controls in a risk event

A common control is automatically linked to a risk event when the underlying risk has materialized for the risk event. It enables the control owner to identify when the common

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

control fails and to take immediate action if a common control does fail. The following example shows the inherit common controls option on the risk event form:

**Common controls in risk event**




Related topics

Add a control to a risk

Associate a risk statement with a control objective

## Create and run a manual risk indicator in the Risk Workspace

Create and run a manual risk indicator to identify the possibility of a future adverse impact on your organization. Indicators are an early warning system and they enable you to take preventative actions on risks. In a manual indicator, the results are manually gathered using task assignments.

### Before you begin

Role required: sn_risk.manager or sn_risk.admin

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Indicators** > **Risk indicators**.
2. Click **New**.
3. On the form, fill in the fields.

**Indicator form**

| Field | Description |
|---|---|
| Category | Category of the indicator. For example, select **Risk Indicator** to create a risk indicator. |
| Inherit from template | Option to create the indicator from an existing template. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Template | Template used to create the indicator. This field appears only if the **Inherit from template** option is selected. |
| Override template | Option to override the template's properties such as the name of the indicator. |
| Name | Name of the indicator. If you select a template in the **Template** field, then this field is automatically set to the template name. |
| Description | Brief description of the indicator. This field is automatically set if you select a template in the **Template** field. |
| Entity | Entity used to filter risks. |
| Applies to record | Record that the entity applies to. This field is automatically set. |
| Risk | Filtered risk that is related to the indicator.<br>**Note:** If you have selected an indicator template, then the risk is also filtered based on the template. |
| Owning group | Group that owns the indicator. This field is automatically set based on the owning group of the risk. |
| Owner | Owner of the indicator. This field is automatically set to the owner's name based on the risk. |
| Method | |
| Type | Method used to determine the type of indicator. Select **Manual**. |
| Target type | Type of the target value. Choices are as follows:<br>◦ **None**: Use this option if you do not want to set up any target or threshold for the indicator.<br>◦ **Percentage**: Use this option to determine the indicator result by a percentage value.<br>◦ **Count**: Use this option to determine the indicator result by a count value or total number. |
| Value mandatory | Option to decide if a value is required in the indicator task for a manual indicator. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** This option is automatically selected when **Count** or **Percentage** is selected from the **Target type** field. |
| Target | Numerical value that is your goal for the indicator. This value determines if the indicator succeeded (passed) or failed. For example, if your goal for employee retention is 80%, you can enter the goal as the value. Any result less than 80% would mean the indicator failed. |
| Result if the value meets or exceeds the target value | Result configuration field. The choices are as follows:<br>◦ **Passed**<br>◦ **Failed**<br>For example, assume you enter `80` in the **Target** field. If the indicator result output is more than 80, then the **Indicator status** field is set to **Passed** or **Failed** based on the value configured in the **Result based on target value** field. |
| Instructions for collecting data | More instructions on how to collect data. |
| Reference field | Connection between the supporting data table and the **Applies to record** field of the entity. |
| Basic Criteria | |
| **Note:** This section appears only after you specify supporting data. | |
| Criteria | Criteria to filter the data from the source table. Click **Set conditions** inside the field and create filters for the conditions. |
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| First run date | Date the indicator was first run. |
| Next run date | Next collection time for indicator results. This field is automatically set based on the value in the **Collection frequency** field. You can also edit this field and change the date. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** This field only gets updated based on the scheduled runs and not when the indicators are manually executed. |
| Results | |
| Status | Status of the indicator to show whether the indicator passed or failed. |
| Previous status | Previous status of the indicator to show whether the indicator passed or failed. |

4. Click **Save**.
5. To collect supporting data, click **Specify supporting data** and do the following:
   a. In the **Source table** field, select the table used for collecting supporting data.
   b. In the **Supporting data fields** field, select the fields of the source table that are used for collecting the supporting data.
   While specifying the supporting data fields, you cannot dot-walk in the Risk Workspace.
   c. In the **Sample size** field, specify the minimum number of records that must be used for collecting supporting data.
   d. Click **Save** and reload the form.
6. Click **Execute**.
   An indicator task is created and assigned to the risk owner. After the risk owner closes the indicator task, the Indicator Results related list appears.
7. To see the results of the indicator task, click the Indicator Results related list and do the following:
   a. Click the result that you want to view.
   b. To view the snapshot of the supporting data, click **View supporting data**.
   c. To view a particular live record, click **View** for that record.
   Live records always open in the classic user interface and not in the Risk Workspace user interface.

## Create and run a basic risk indicator in the Risk Workspace

Create and run a basic risk indicator to identify the possibility of a future adverse impact on your organization. Indicators are an early warning system and they enable you to take preventative action on the risks. Basic indicators are automated indicators based on an indicator source.

### Before you begin

Role required: sn_risk.manager or sn_risk.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

In a basic indicator, the data is automatically collected from the source you specify. You must specify the supporting data before adding the criteria to filter data.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Indicators** > **Risk indicators**.
2. Click **New**.
3. On the form, fill in the fields.

**Indicator form**

| Field | Description |
|---|---|
| Category | Category of the indicator. For example, select **Risk Indicator** to create a risk indicator. |
| Inherit from template | Option to create the indicator from an existing template. |
| Template | Template used to create the indicator. This field appears only if the **Inherit from template** option is selected. |
| Override template | Option to override the template's properties such as the name of the indicator. |
| Name | Name of the indicator. If you select a template in the **Template** field, then this field is automatically set to the template name. |
| Description | Brief description of the indicator. This field is automatically set if you select a template in the **Template** field. |
| Entity | Entity used to filter risks. |
| Applies to record | Record that the entity applies to. |
| Risk | Filtered risk that is related to the indicator.<br>**Note:** If you have selected an indicator template, then the risk is also filtered based on the template. |
| Owning group | Group that owns the indicator. |
| Owner | Owner of the indicator. This field is automatically set to the owner's name based on the risk. |
| Method | |
| Type | Method used to determine the type of indicator. Select **Basic**. |
| Target type | Type of the target value. The choices are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ **None**: Use this option if you do not want to set up any target or threshold for the indicator.<br>◦ **Percentage**: Use this option to determine the indicator result by a percentage value.<br>◦ **Count**: Use this option to determine the indicator result by a count value or total number. |
| Target | Value that determines if the indicator succeeded (passed) or failed. |
| Result based on target value | Result configuration field. The choices are as follows:<br>◦ **Passed**<br>◦ **Failed**<br>For example, assume you enter `100` in the **Target** field. If the indicator result output is more than 100, then the indicator status is **Passed** or **Failed** based on the value configured in this field. |
| Basic Criteria | |
| **Note:** This section appears only after you specify supporting data. | |
| Criteria | Criteria to filter the data from the source table. Click **Set conditions** inside the field and create filters for the conditions. |
| Additional Criteria | |
| Additional criteria | More criteria to filter the data to calculate the target value. This section only appears when **Percentage** is selected from the **Target type** field. Click **Set conditions** inside the field and create filters for the conditions. |
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| First run date | Date the indicator was first run. |
| Next run date | Next collection time for indicator results. This field is automatically set based on the value in the **Collection frequency** field. You can also edit this field and change the date. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** This field only gets updated based on the scheduled runs and not when the indicators are manually executed. |
| Results | |
| Status | Status of the indicator to show whether the indicator passed or failed. |
| Previous status | Previous status of the indicator to show whether the indicator passed or failed. |

4. Click **Save**.
5. To collect supporting data, click **Specify supporting data** and do the following:
   a. In the **Source table** field, select the table used for collecting supporting data.
   b. In the **Supporting data fields** field, select the fields of the source table that are used for collecting the supporting data.
   While specifying the supporting data fields, you cannot dot-walk in the Risk Workspace.
   c. In the **Sample size** field, specify the minimum number of records that must be used for collecting supporting data.
   d. Click **Save** and reload the form.
6. Click **Execute**.
   The Indicator Results related list appears.
7. To see the results of the indicator, click the Indicator Results related list and do the following:
   a. Click the result that you want to view.
   b. To view the snapshot of the supporting data, click **View supporting data**.
   c. To view a particular live record, click **View** for that record.
   Live records always open in the classic user interface and not in the Risk Workspace user interface.

## Create and run a scripted risk indicator in the Risk Workspace

Create and run a scripted risk indicator to identify the possibility of a future adverse impact on your organization. A scripted indicator enables you to write your own script to run the indicators. Indicators are an early warning system and they enable you to take preventative action on the risks.

### Before you begin

Role required: sn_risk.manager or sn_risk.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Indicators** > **Risk indicators**.
2. Click **New**.
3. On the form, fill in the fields.

### Indicator form

| Field | Description |
|---|---|
| Category | Category of the indicator. For example, select **Risk Indicator** to create a risk indicator. |
| Inherit from template | Option to create the indicator from an existing template. |
| Template | Template used to create the indicator. This field appears only if the **Inherit from template** option is selected. |
| Override template | Option to override the template's properties such as the name of the indicator. |
| Name | Name of the indicator. If you select a template in the **Template** field, then this field is automatically set to the template name. |
| Description | Brief description of the indicator. This field is automatically set if you select a template in the **Template** field. |
| Entity | Entity used to filter risks. |
| Applies to record | Record that the entity applies to. |
| Risk | Filtered risk that is related to the indicator.<br>**Note:** If you have selected an indicator template, then the risk is also filtered based on the template. |
| Owning group | Group that owns the indicator. |
| Owner | Owner of the indicator. This field is automatically set to the owner's name based on the risk. |
| Method | |
| Type | Method used to determine the type of indicator. Select **Script**.<br>**a.** To add your script, save the form and click **Add script**.<br>**b.** Click **Save**. |
| Target type | Type of the target value. The choices are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ **None**: Use this option if you do not want to set up any target or threshold for the indicator.<br>◦ **Percentage**: Use this option to determine the indicator result by a percentage value.<br>◦ **Count**: Use this option to determine the indicator result by a count value or total number. |
| Target | Value that determines if the indicator succeeded (passed) or failed. |
| Schedule | |
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule. |
| First run date | Date the indicator was first run. |
| Next run date | Next collection time for indicator results. This field is automatically set based on the value in the **Collection frequency** field. You can also edit this field and change the date.<br>**Note:** This field only gets updated based on the scheduled runs and not when the indicators are manually executed. |
| Results | |
| Status | Status of the indicator to show whether the indicator passed or failed. |
| Previous status | Previous status of the indicator to show whether the indicator passed or failed. |

4. To collect supporting data, save the form and click **Specify supporting data** and do the following:

   a. In the **Source table** field, select the table used for collecting supporting data.

   b. In the **Supporting data fields** field, select the fields of the source table that are used for collecting the supporting data.
   While specifying the supporting data fields, you cannot dot-walk in the Risk Workspace.

   c. Click **Save** and reload the form.

5. Click **Execute**.
   The Indicator Results related list appears.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. To see the results of the indicator, click the Indicator Results related list and do the following:

   a. Click the result that you want to view.

   b. To view the snapshot of the supporting data, click **View supporting data**.

   c. To view a particular live record, click **View** for that record.
   Live records always open in the classic user interface and not in the Risk Workspace user interface.

## Issue management in the Risk Workspace

The issues landing page in the Risk Workspace provides logged-in managers and users with all the information they need to manage issues on a single page. The landing page features actionable insights, quick action buttons, filters, and access to open issue triages.

The issues landing page is available in the following workspaces:

- Compliance Workspace
- Audit Workspace
- Privacy Workspace
- Risk Workspace

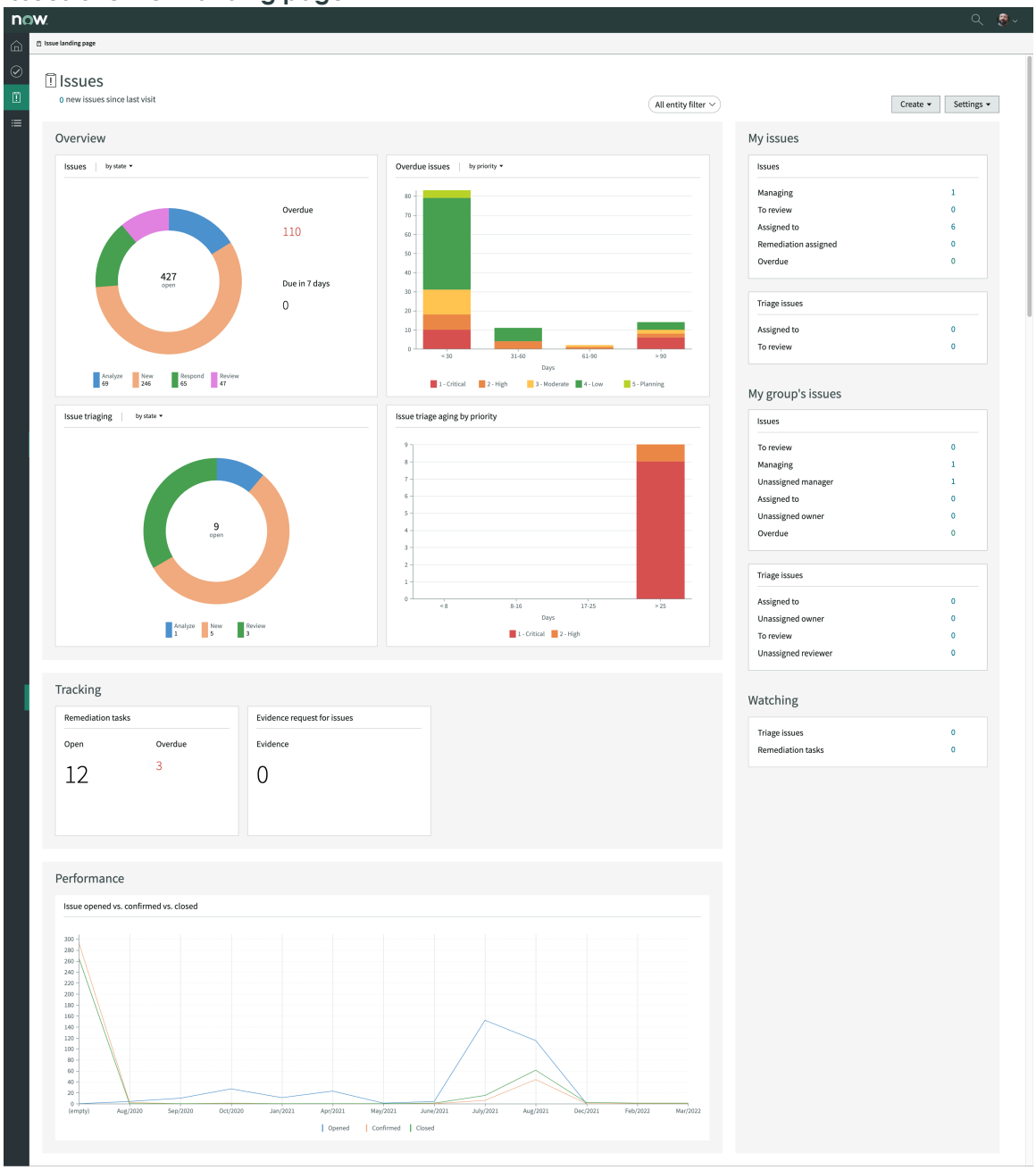
## Open the Issues overview landing page

On each of the listed workspaces, you can access the issues by clicking the Issue overview icon (  ).

Click this icon to open the Issues overview landing page.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Issues overview landing page




## Sections of the Issues overview landing page

### Charts and graphs on the Issues overview landing page

| Overview | |
|---|---|
| Issues | This chart shows issues broken down by state, issue type, issue rating, or priority. The number of overdue issues and issues due in seven days are also shown. |
| Overdue issues | This aging chart shows issues overdue by different ranges of time. For example, you can determine, at a glance, issues that are between 61 and 90 days overdue. The chart can be filtered by priority and issue rating. |
| Issue triaging | This chart shows issue triages by state, issue type, or priority. It can aid issue managers identify how issues are being triaged and prioritized. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Charts and graphs on the Issues overview landing page (continued)**

| | |
|---|---|
| Issue triage aging by priority | This aging chart provides an overview of how long issues have been open. |
| Tracking | |
| Remediation tasks | This widget shows the status of open and overdue remediation tasks associated with issues. |
| Evidence request for issues | This widget shows the number evidence requests that have been opened for issues. |
| Performance | |
| Issue opened vs. confirmed vs. closed | This chart shows trend data for open, confirmed, and closed issues over time. |
| My issues | |
| Issues | The section shows issues assigned to the logged-in user that can be reviewed, re-assigned, assigned for remediation, and that are overdue. |
| Triage issues | The section shows triage issues assigned to the logged-in user that can re-assigned and reviewed. |
| My group's issues | |
| Issues | The section shows issues assigned to member of the logged-in user's group. |
| Triage issues | The section shows triage issues assigned to the logged-in user's group. |
| Watching | |
| Triage issues | This section shows the number of triage issues for which the logged-in user is on the watch list. |
| Remediation tasks | This section shows the number of remediation tasks for which the logged-in user is on the watch list. |

## Create a risk assessment scope in the Risk Workspace

Create a risk assessment scope to identify risks for an entity, define assessors and approvers, set assessment frequency, and initiate assessments using the Risk Management application.

### Before you begin

Role required: sn_risk_workspace.IT_risk_manager, sn_risk_workspace.operational_risk_manager, or sn_risk_workspace.business_op_risk_manager

### About this task

Creating a risk assessment scope ensures that assessments are effectively carried out, resulting in valuable insights for the risk management team and enabling informed decision-making. You can create a risk assessment scope with a guided experience using the playbook. Each stage within the playbook includes one or more activities that must be completed, providing a structured approach to the risk assessment scope. The playbook guides you through each stage, recommending necessary activities, and ensuring comprehensive coverage of the workflow. Stages can also include automated activities, such as auto-sending an email to the Assessor when you initiate an assessment.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace**.
2. Select the list  icon.
3. From the list, navigate to **Risk assessment planning** select **Scoped entities**.
4. Select **New**.
   The Risk assessment scope playbook opens and initiates the first activity for defining the risk assessment methodology (RAM) and assessable entity, which is the Scope definition stage.
5. On the Scope definition activity card, fill in the fields.

### Scope definition card

| Field | Description |
|---|---|
| Risk assessment methodology | Risk assessment methodology (RAM) that you use to assess risks. |
| Assessable entity | Entities associated with the selected entity classes defined in the **Applicable entity classes** field on the RAM. The value of this field changes based on the entity classes specified in your selected RAM. Only those entities that belong to the selected classes are displayed in this field. |
| Owner | Owner of the entity. This field is automatically set based on the assessable entity. |

6. Select **Continue**.
   The Risks selection activity card opens that enables you to select and assess the risks related with the entity using the selected RAM.
7. To add existing risks, select **Add** and do the following:
   a. Select the risks to add.
   b. Select **Add**.
8. Optional: To create risks, select **Create risk** and do the following:
   a. Fill in the details of the new risk.
   b. Select **Save**.
9. Optional: To create risks from the risk taxonomy, select the down arrow icon next to the **Create risk** button, select **Create from risk statements**, and do the following:
   a. Select the risk statements to add.
   b. Select **Add**.
10. Select **Mark as complete**.
    The Assignment stage in the Risk assessment scope playbook opens.
11. On the Assignment activity card, fill in the fields.

### Assignment card

| Field | Description |
|---|---|
| Assessor type | User or group who is responsible for assessing the risk. Choices are as follows:<br>◦ **Same as entity owner**<br>◦ **Same as risk owner** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ **Specify users**<br>◦ **Specify groups** |
| Assessor | User who is responsible for assessing the risk. This field appears only when **Specify users** is selected from the **Assessor type** field. |
| Assessor group | Group that is responsible for assessing the risk. This field appears only when **Specify groups** is selected from the **Assessor type** field. |
| Approver type | User or group who is responsible for approving the assessment. Choices are as follows:<br>◦ Same as entity owner<br>◦ Same as assessor's manager<br>◦ Specify users<br>◦ Specify groups<br>◦ None |
| Approver | User who is responsible for approving the assessment. This field appears only when **Specify users** is selected from the **Approver type** field. |
| Approver group | Group that is responsible for approving the assessment. This field appears only when **Specify groups** is selected from the **Approver type** field. |

12. Select **Mark as complete**.
    The Reassessment frequency stage in the Risk assessment scope playbook opens.
13. On the Reassessment frequency activity card, fill in the fields.

**Reassessment frequency card**

| Field | Description |
|---|---|
| Reassessment frequency | How often you want to assess risks. Choices are as follows:<br>◦ None<br>◦ Weekly<br>◦ Monthly<br>◦ Quarterly<br>◦ Semi-annually<br>◦ Annually<br>**Note:** If you conduct an unplanned risk assessment before the next scheduled reassessment date, the subsequent assessment date is determined by the frequency established in the last assessment. For example, if your frequency is set as monthly and you conduct the initial assessment on January 1. Then, if you perform an unplanned assessment on January 15, the next assessment will still be based on the last assessment date. |
| Days to overdue | Number of days within which the assessment should be completed after it is initiated. For example, if you define a value of 10 in this field, |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | the due date of the assessment will be set to 10 days after the date the assessment is initiated. The default value is 5. |

14. Select **Mark as complete**.
    The Initiate assessments stage in the Risk assessment scope playbook opens.
15. To initiate the assessments, select **Initiate all assessments**.
    When you generate an assessment, the assessor or the assessor's group gets an email notification indicating that the assessment has been assigned to them.
16. Optional: To go back in the workflow and change the scope, assignment, or frequency, select ⋮ and then select **Redefine scope**.

## Schedule risk assessments in the Risk Workspace

Schedule risk assessments automatically for multiple entities. The risk assessment scheduler helps the risk administrators save time by automatically initiating the assessments based on the frequency that you want.

### Before you begin

Role required: sn_risk_workspace.IT_risk_manager and sn_risk_workspace.operational_risk_manager

### About this task

In most organizations, the second line of risk managers is responsible for coordinating risk assessments. This group identifies the entities and associated risks that require assessment. They also determine the individuals responsible for assessing these risks. However, this continuous cycle of risk assessment demands that risk managers create individual risk assessment scopes and initiate assessments, leading to a significant loss of their time. To address this issue, the risk assessment scheduler can be utilized. By utilizing the scheduler, you have the ability to schedule assessments and specify their frequency. The system will automatically initiate the assessments based on the defined frequency. Additionally, you can designate the assessors and approvers for each assessment.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace**.
2. To access the Assessment scheduler playbook, do any of the following:
   - On the Risk Workspace home page, under **Quick actions**, select **Schedule risk assessments**.
   - Select the list icon, navigate to **Risk assessment planning**, select **Scheduled assessments**, and select **New**.

   The Assessment scheduler playbook opens and initiates the first activity for defining the risk assessment methodology (RAM) and assessable entities, which is the Scope definition stage.
3. On the Scope definition activity card, fill in the fields.

#### Scope definition card

| Field | Description |
|---|---|
| Risk assessment methodology | Risk assessment methodology (RAM) that you use to assess risks. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Applicable entity classes | Entity classes related to the selected RAM. The value of this field changes based on the entity classes specified in your selected RAM. This field is automatically set based on the applicable entity classes for the selected RAM. |

4. Select **Continue**.
   The entity selection activity card opens up, enabling you to add the assessable entities that belong to the applicable entity classes.
5. To add entities, select **Add** and do the following:
   a. Select the entities to add.
   b. Select **Add**.
6. Select **Mark as complete**.
   The Assignment stage in the Assessment scheduler playbook opens.
7. On the Assignment activity card, fill in the fields.

### Assignment card

| Field | Description |
|---|---|
| Assessor type | User or group who is responsible for assessing the risk. Choices are as follows:<br>◦ Entity owners<br>◦ Risk owners<br>◦ Group |
| Assessor group | Group that is responsible for assessing the risk. This field appears only when **Group** is selected from the **Assessor type** field. |
| Approver type | User or group who is responsible for approving the assessment. Choices are as follows:<br>◦ Entity owners<br>◦ Assessor's manager<br>◦ Group<br>◦ None |
| Approver group | Group that is responsible for approving the assessment. This field appears only when **Group** is selected from the **Approver type** field. |

8. Select **Mark as complete**.
   The Reassessment frequency stage in the Assessment scheduler playbook opens.
9. On the Reassessment frequency activity card, fill in the fields.

### Reassessment frequency card

| Field | Description |
|---|---|
| Initiate later | Option to initiate the assessments on a future date. |
| Initiate assessments on | Date on which you want to schedule an assessment. This field appears only when the **Initiate later** option is selected. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Reassessment frequency | How often you want to assess risks. Choices are as follows:<br>◦ None<br>◦ Weekly<br>◦ Monthly<br>◦ Quarterly<br>◦ Semi-annually<br>◦ Annually<br>**Note:** If you conduct an unplanned risk assessment before the next scheduled reassessment date, the subsequent assessment date is determined by the frequency established in the last assessment. For example, if your frequency is set as monthly and you conduct the initial assessment on January 1. Then, if you perform an unplanned assessment on January 15, the next assessment will still be based on the last assessment date. |
| Days to overdue | Number of days within which the assessment should be completed after it is initiated. For example, if you define a value of 10 in this field, the due date of the assessment will be set to 10 days after the date the assessment is initiated. The default value is 30. |

10. Select **Mark as complete**.
    The Review and initiate stage in the Assessment scheduler playbook opens.
11. To initiate the assessments, select **Initiate assessments**.
    When you generate an assessment, the assessor or the assessor's group gets an email notification indicating that the assessment has been assigned to them.
12. Optional: To go back in the workflow and change the scope, assignment, or frequency, select ⋮ and then select **Redefine scope**.

**Result**
The assessments are initiated. You can view all the scheduled assessments under **Risk assessment planning** > **Scheduled assessments**.

## Perform advanced risk assessment in the Risk Workspace

Conduct risk assessments to assess inherent risks, effectiveness of controls, residual risks, and target risks in the Risk Workspace application. You can define risk responses that enable you to manage and mitigate the risks identified during the risk assessment process.

**Before you begin**
Role required: sn_grc.business_user

**Note:** You must manually assign the advanced risk assessment roles to the sn_grc.business_user role. To understand how you can adjust the granting of roles and groups, see the How to adjust granting of roles and groups to use background jobs [KB0963693] article in the Now Support Knowledge Base. You must log in to Now Support to view the article.

**About this task**
A risk assessment is performed for the following:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Inherent risks
- Effectiveness of controls
- Residual risks
- Target risks

The risk assessments yield risk scores that are automatically calculated based on the configurations made in the risk assessment methodology (RAM). If you want to change the automatically calculated scores, you can overwrite the calculated scores and provide a justification. If you have no controls to assess, then the residual risk score is the same as the inherent risk score.

After performing the assessment, you can define the risk response. Risk response refers to the process of managing identified risks. It's a planning and decision-making process where the risk managers decide how to deal with each risk. While performing the assessment, you can view detailed reference information on the Contextual side panel. This panel provides information for the risk events, open issues, key indicator breaches, control test results, and control indicator failures.

If the risk assessment in being performed by an assessor's delegate, the **Assessor's delegates** field shows the delegate's name.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **My tasks**.
2. Open the risk assessment that you want to assess and do one of the following.
   - If you want to start the assessment, select **Let's get started**.
   - If you think that the risk assessment must be assigned to someone else, select **Reassign** and fill in the necessary details.
   - If this risk was previously assessed, to view the previous assessment, select **Review last assessment**.
3. To perform inherent assessment, respond to the all inherent assessment questions.
   a. Optional: To view the guidance for a factor, select the question mark icon ( .
   b. Optional: To view the qualitative and quantitative weightage, select overall rating icon.
   The application automatically saves your responses and calculates the overall risk score.
4. Optional: To change the computed inherent risk results, do the following:
   a. Select the **I would like to change the computed score** option.
   b. From the **Override inherent risk** field, select the appropriate value.
   c. Enter comments that explain the reasons for the change in the computed score.
5. Select **Move to control assessment**.
6. For the Control assessment, do one of the following:
   - To assess the effectiveness of the controls, respond to all the control assessment factors.
   - To proceed without assessing the mitigating controls, select the **Control assessment not applicable** option.
   - To assess the control environment without adding controls, select **I would like to change the computed score** option and refer to step 8.

   You can also change the computed control effectiveness results by providing a justification for changing the score.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

7. To add or create controls for the control assessment, do one of the following:
   - To add existing controls, select **Add**.
   - To inherit common controls, select **Inherit common controls**.
   - To create a control, select the down-arrow next to the **Inherit common controls** button, and select **Create control**.
   - To add controls from control taxonomy, select the down-arrow next to the **Inherit common controls** button, and select **Create from control objectives**.
8. Optional: To assess the control environment without adding controls, do the following:
   a. Select the **I would like to change the computed score** option.
   b. From the **Override control effectiveness** field, select the appropriate value.
   c. Enter comments that explain the reasons for the change in the computed score.
9. To assess the leftover risks after the implementation of mitigating controls, select **Move to residual assessment** and respond to the factors.
   You can also change the computed residual score by providing a justification for changing the score.
10. **Note:** The availability of the target risk assessment on the assessment form depends on the conditions outlined in the RAM.

    To assess the desired risk level that you want to achieve in the future, select **Move to target assessment** and respond to the factors.
    You can also change the computed target score by providing a justification for changing the score.
11. To select an appropriate strategy and to define the plan of action for the risks assessed, do the following.
    a. Select **Define risk response**.
    b. Select the appropriate risk responses.
    c. Optional: To create a risk response task, select the **Create task** button, and select the appropriate values.
    d. Select **Review and submit** and review your responses.
       The risk response tasks are created and assigned to the assignee. You can edit the task and modify it to change the owner.
12. Optional: If you want to modify the assessment, select **Edit**.
13. Optional: To view the activities taking place for the assessment, select the Activity log icon .
14. If you have defined approvers, then select **Submit**.
    The assessment home page is displayed. You can review the summary of your assessment.
15. To request approval, edit assignment, or reassign, select one of the following.

| Choice | Description |
| --- | --- |
| Request approval | If an approver is specified, select this option to send the assessment for approval. You |

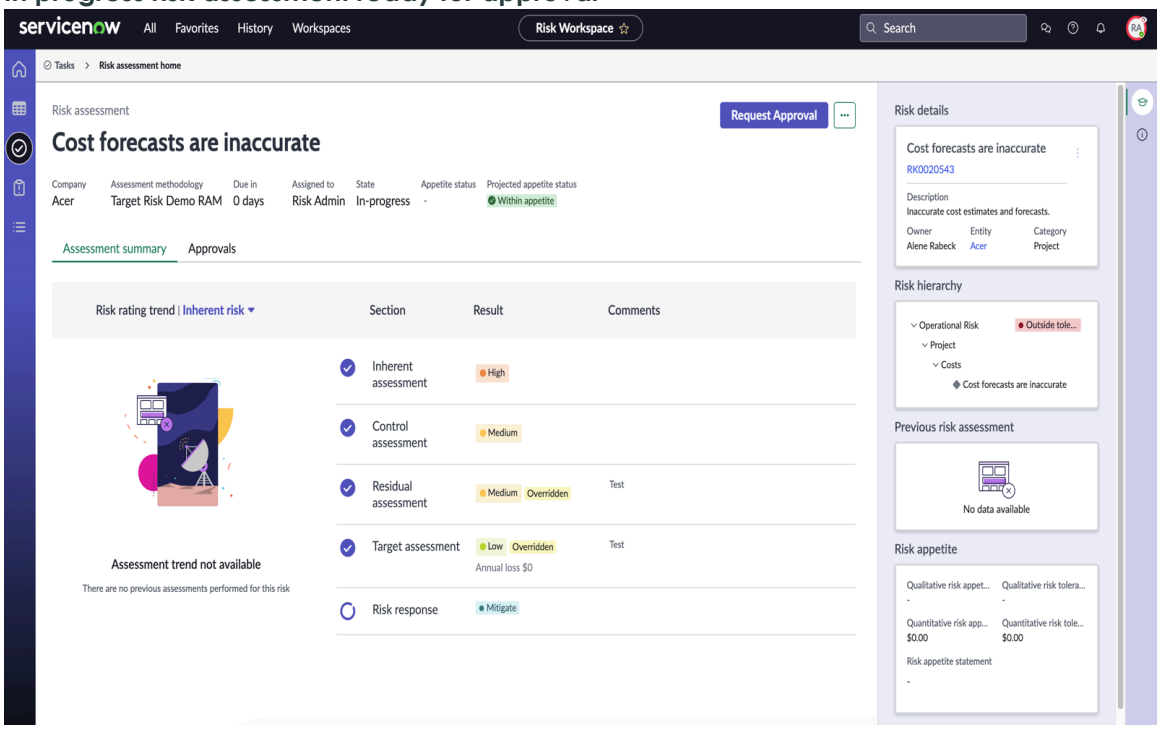
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Choice | Description |
|---|---|
| | can also provide additional comments for the approver. |
| Edit assessment | If you want to modify your responses in the assessment, select this option. |
| Reassign | If the assessment must be assigned to some-one else, select this option. |

**Result**
The assessment is sent to the approver and the approval workflow starts.

**Example:**

**In progress risk assessment ready for approval**




## Perform any object assessment in the Risk Workspace

Assess the risks on any object or record in ServiceNow®. An example of object assessment is assessing change management or assessing a citation.

**Before you begin**
Role required: sn_grc.business_user

**About this task**
To perform an object risk assessment, a prior knowledge of risk is not necessary. When you perform any object assessment in the Risk Workspace, you do not see the description of the risk and any reference information because the entire context of risk is not required. You can configure the risk assessment button in the object record and start the assessment. For more information, see Any object assessment using Advanced Risk Assessment.

**Procedure**

1. Navigate to my **All** > **Risk** > **Risk Workspace**.
2. Click the Work queue ( )

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Under **My pending tasks**, under Advanced risk assessments, open the object risk assessment assigned to you.

| Choice | Description |
|---|---|
| Start assessment | Select this option if you want to proceed with the assessment. |
| Reassign | Select this option if the assessment must be assigned to someone else. |

4. If you select **Start assessment**, respond to the assessment questions.
   For more information, see Perform advanced risk assessment in the Risk Workspace.
5. Click **Save**.
6. If you have configured risk response in your risk assessment methodology, select the appropriate risk response strategy and click **Define risk response**.
7. To send the assessment for review, click **Review and submit**.
   The assessment home page is displayed. You can review the summary of your assessment.
8. To request approval, edit assignment, or reassign, select one of the following. **Request approval**.

| Choice | Description |
|---|---|
| Request approval | Select this option to send the assessment for approval if an approver is specified. If you select this option, you can provide additional comments for the reviewer. |
| Edit assignment | Select this option if you want to modify your responses in the assessment. |
| Reassign | Select this option if the assessment must be assigned to someone else. |

## Workflow for risk identification in the Risk Workspace

Workflows provide step-by-step guidance for completing the risk identification process in the GRC Risk Workspace.

In the Risk Workspace, a risk manager can use the risk identification workflow to identify risks. The workflow has multiple stages. The stage progress gets updated as activities are completed. The risk identification workflow is broken it into multiple lanes. Each lane in the workflow includes one or more activities for a task owner to complete.

The benefit of using the risk identification workflow is that you can get a detailed view on a single interface. You can also easily go back to any stage and restart an activity.

For risk identification, after a risk identification record is created, the information gathering questionnaire is sent to the assigned user. You can also send email reminders to the users to respond to the questionnaire. After the responses are received, the risk manager can do the following activities:

1. View the responses.
2. Approve or reject the responses.

> **Note:** If there is rejection, the risk manager can provide a reason for rejection and resend the questionnaire.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Initiate inherent assessment.
4. Perform the risk assessment.
5. View the assessment scores.
6. Relate either the recommended risks or relate them from the library. Alternatively, the risk manager can also create risks.

   **Note:** Recommended risks are risks that are generated from information objects.

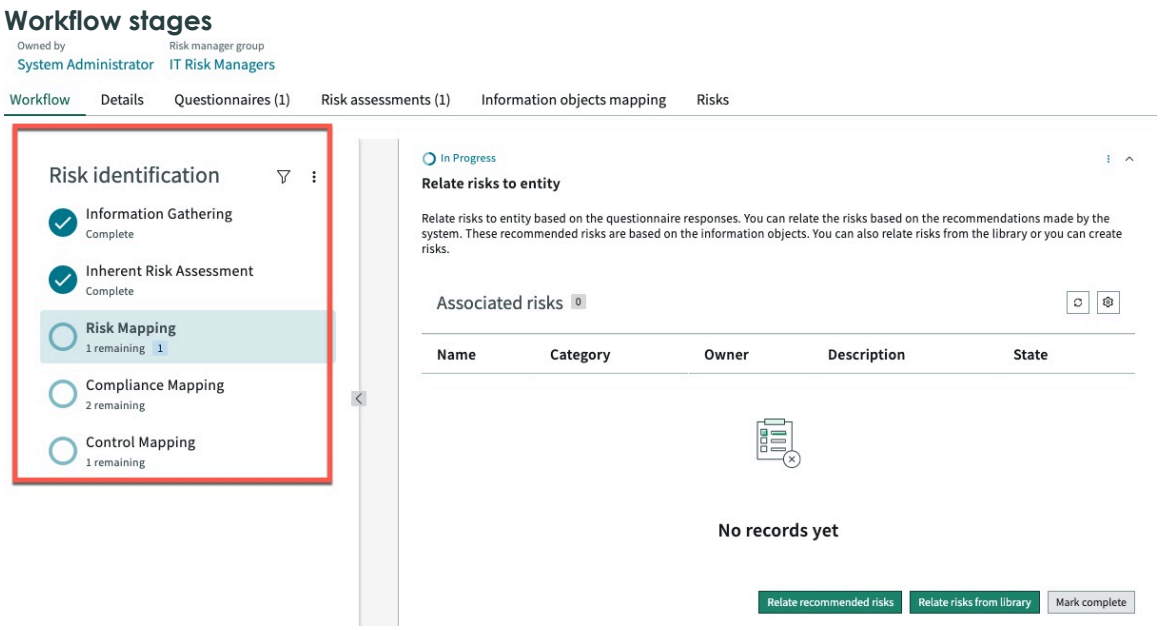
7. Mark the activity as complete.
8. Relate either the recommended policies or relate them from the library.
9. Relate or create additional controls after the controls for various risks and policies are automatically generated.
10. Request attestations for either all the controls or selective controls.

It is important to remember the following points:

- In a workflow, the stage progression is automatic, however, if you restart any activity after completing it, you have to manually move to the next stage.
- If you finish relating the controls and then again move to risk mapping, the control-mapping stage moves to pending state.
- When you reinitiate a workflow, a new workflow instance is created.

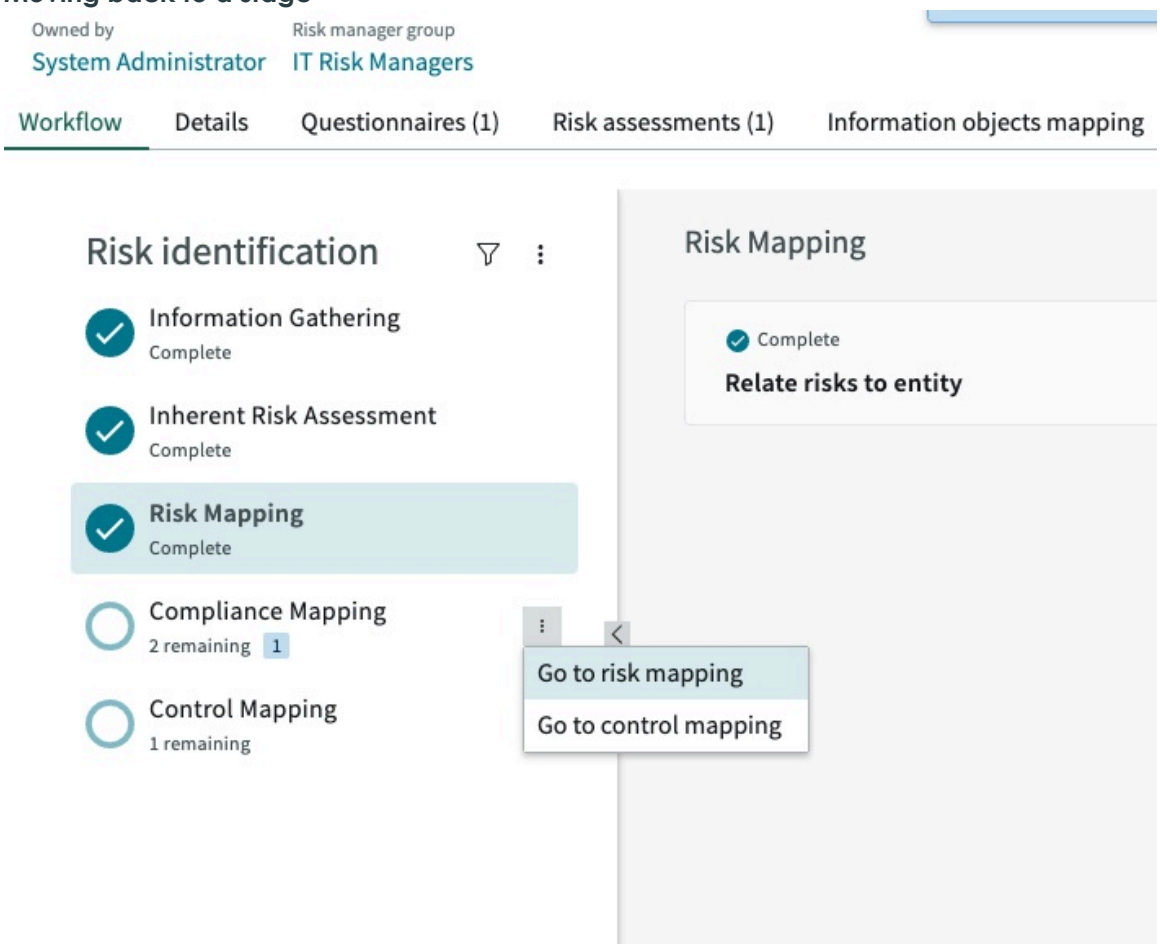
For more information, see Application risk assessment using advanced risk assessment

The following figures show the workflow stages and actions:

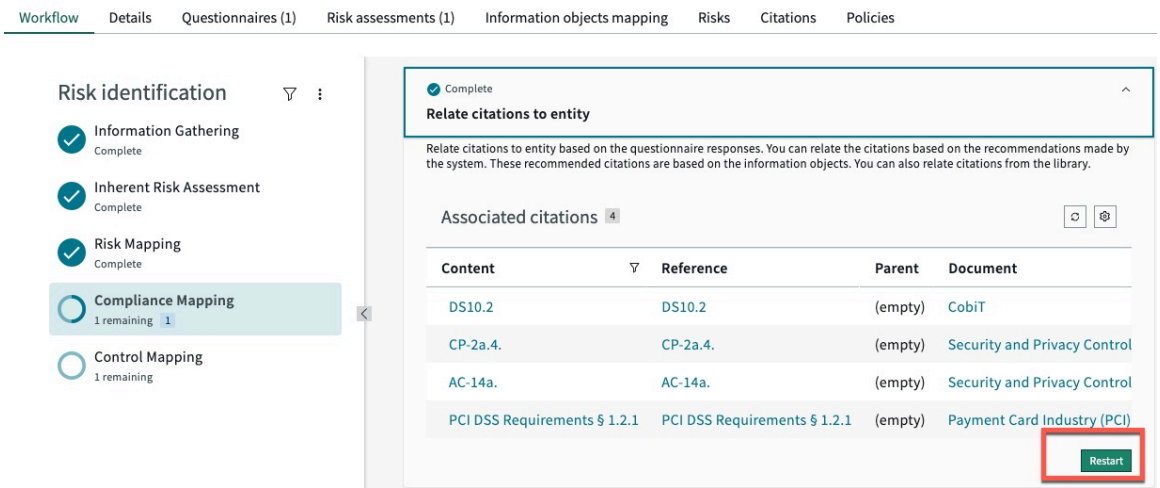



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Moving back to a stage




### Restarting an activity




## Create a risk event in the Risk Workspace

Create a risk event in the Risk Workspace. Risk events are potential or actual financial and non-financial losses, near misses, and gains that occur within an organization.

**Before you begin**
Role required: sn_risk.manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

When you create a risk event, the risk event goes through the defined lifecycle of analysis, approval, and closure. Creating or recording risk events enables your organization to prevent similar events from occurring.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Risk events** > **All events**.
2. Click **New**.
3. On the form, fill in the following fields:

**Create New Risk Event form**

| Field | Description |
|---|---|
| Name | Name of the risk event such as `ATM Theft`. |
| Description | Description of the risk event reported. |
| Classification | |
| Event type | Type of event. The options are as follows:<br>◦ **Financial Impact**: Select this option when the event leads to monetary losses.<br>◦ **Non-Financial Impact**: Select this option when the event does not have monetary losses. |
| Category | Event category. You can edit the category to apply one of the following options:<br>◦ **Personal**: For example, any physical harm caused to an employee.<br>◦ **Legal**: For example, an employee is found conducting business that is a conflict of interest.<br>◦ **Information Security**: For example, a theft, burglary, or system crash.<br>◦ **Human Resources**: For example, sensitive lawsuits by an employee against another employee. |
| Sub type | Event sub type. The choices are as follows:<br>◦ **Actual**: Select this option if the event has actually occurred.<br>◦ **Potential**: Select this option if the event has the potential to occur. |
| Discovered by | Person who discovered the risk event. |
| Opened | Date of risk event creation. |
| Opened by | Person creating the risk event. |
| Near miss | Option to specify if the risk event had the potential to incur losses but did not result in losses. This field is available when **Potential** is selected from the **Sub type** field. |
| Financial gain | Option to show if the risk event resulted in a gain instead of a loss. This option is automatically selected if the risk event meets one of the following conditions: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ If **Potential** is selected from **Sub type** field and the **Expected loss** field or the **Potential loss** field has a negative value because of the gain.<br>◦ If **Actual** is selected from **Sub type** field and the **Net loss** field has a negative value. |
| Used in modeling | Option to share the risk event records with external systems where advanced analysis is performed using simulation techniques such as the Monte Carlo simulation. The Monte Carlo simulation is a mathematical technique used to estimate the possible outcomes of an uncertain event. |
| Ownership | |
| Primary entity | Entity that bears the loss. This entity is visible to management for reporting. |
| Owning group | Group responsible for monitoring the event to closure. |
| Cost center | Account number of the entity. |
| Owner | Person who owns the risk event. A risk manager can be an event owner. If the owning group is specified, the owners are filtered from the owning group. |
| Key Dates | |
| Date of occurrence | Date when the event occurred. |
| Date of discovery | Date that the event was first discovered or noticed. |
| Loss/Gain Estimates | |
| Expected loss | Amount of loss expected. Expected loss is the probability weighted average of all possible losses. This amount is based on the user's judgment of the expected amount that the organization might lose. |
| Non financial impact | Rating for the non-financial impact associated with the event. |
| Potential loss | Amount expected to be a potential loss due to the risk event. This amount is the maximum loss an entity can incur due to the loss from the risk event. |
| Credit/Market Risk Overlap | |
| Boundary event | Option to mark the event as a boundary event. A boundary event is an operational risk event which leads to a consequence, such as a financial loss, in another risk category. |
| External risk type | Type of external risk the risk event can have. The choices are as the following:<br>◦ **Credit**: Credit risk is the possibility of a loss resulting from a borrower's failure to repay a loan or meet contractual obligations. For example, when lenders offer credit cards, or loans, there's a risk that the borrower might not repay the loan.<br>◦ **Market**: Market risk is the possibility of an investor incurring losses due to factors that affect the performance of the financial markets in which the investor is involved. For example, a recession might impact the entire market. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | This option appears when **Boundary event** is selected. |
| External risk reference | ID for reconciliation in the book of accounts. This value is automatically set.<br><br>This option appears when **Boundary event** is selected. |
| Root Cause Analysis | |
| Cause | Primary reason why the risk event occurred. |
| Cause description | Brief description about why the risk event occurred. |
| Consequence | Consequence of the risk event. For example, regulatory fines can be imposed as a result of the risk event. |
| Actions taken | Remedial actions that were taken to address the issue. This is the initial record of the event. |
| Activity | |
| Work notes | Notes about the risk event. These notes are not visible to external users. |
| Additional comments | Additional comments about the risk event. These notes are visible to the external users. |

4. Click **Save**.

## Associate similar risk events

Train a similarity solution definition that uses machine learning by activating the Governance, Risk, and Compliance: Predictive Intelligence plugin. The solution enables the system to display similar risk events automatically.

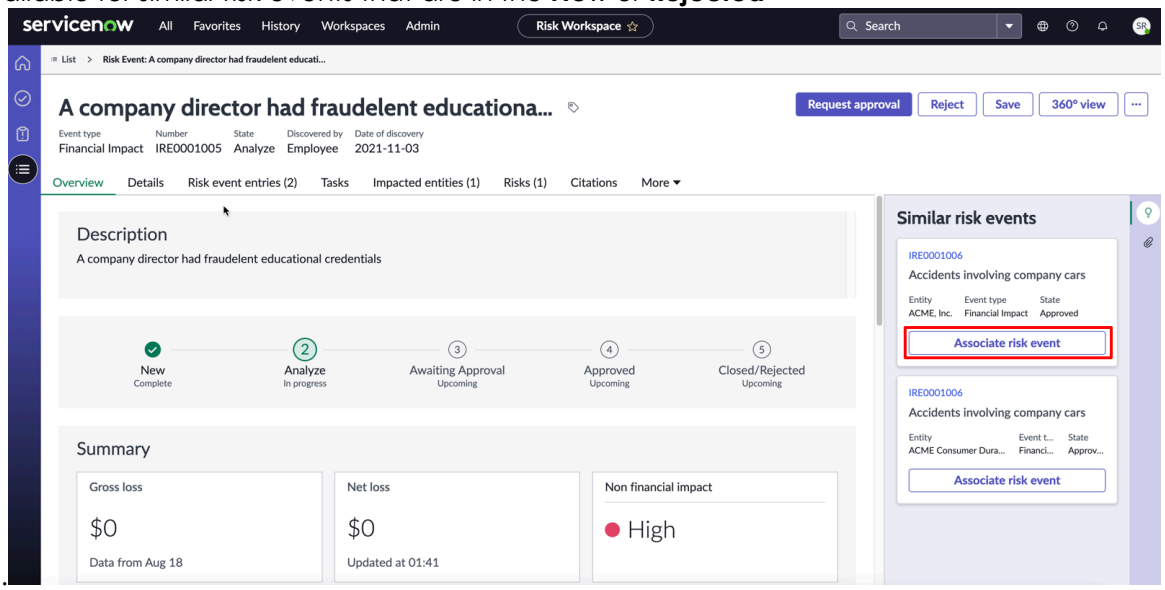
The Governance, Risk, and Compliance: Predictive Intelligence plugin uses Artificial Intelligence (AI) and Machine Learning (ML) to manage the risk events more efficiently. You can identify similar risk events and group them to capture and analyze the actual impact of the risk event.

For example, in an organization with operations in multiple locations, the risk event teams across different locations may be working on similar types of risk events. This challenge results in duplicate efforts to manage the risk events within the organization. This capability reduces the manual effort in managing similar risk events and improves overall organizational efficiency.

You can associate similar risk events only when the main risk event is in the **Analyze** state. Also, the Associate risk event button is

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

unavailable for similar risk events that are in the **New** or **Rejected** state.




The platform machine learning administrator (ml_admin) can create a solution definition and modify an existing one. You can navigate to **Risk Events** > **Administration** > **Properties** to update the risk event property with the new solution definition name.

## Categorizing risks with the Governance, Risk, and Compliance: Predictive Intelligence plugin

By using the Governance, Risk, and Compliance: Predictive Intelligence plugin, you can predict the risk statements for your orphan risks (the risks that don't have risk statements) on the risk records for your organization. You can then identify the correct risk statement for the risks and then aggregate them into manageable categories.

### Overview

Usually, the first line of employees or the risk champions within an organization identify the risks for the business.

**Note:** A risk champion is an executive who is in charge of identifying and reporting risks within an organization.

As the risk champions identify these risks, they manually associate the risks with the correct risk statement. The organization's senior management gets visibility into the organization's risk profile because these operational risks are aggregated into the enterprise risks.

However, your risk champions must manually search the complete risk library to identify the correct risk statement for the identified risks. This activity is time-consuming and is an inefficient use of resources. When the risk champions search for risk statements manually, they tend to select whatever is the earliest match rather than search for the entire library, which results in the incorrect categorization of risks with risk statements.

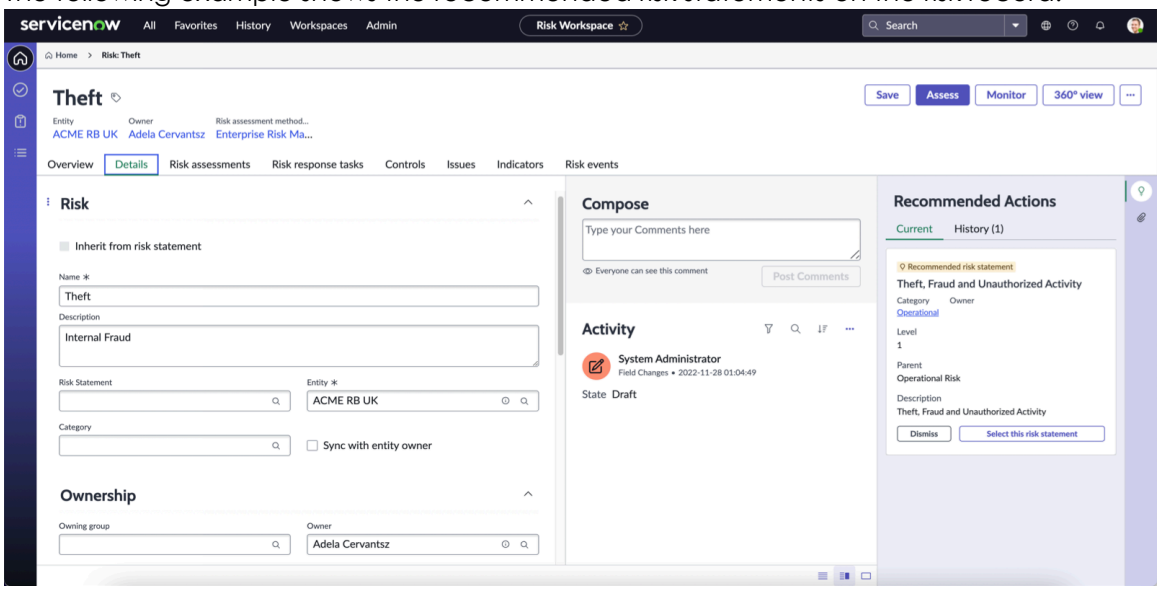
### Predicting risk statements on risk records

The Governance, Risk, and Compliance: Predictive Intelligence plugin uses artificial intelligence (AI) and machine learning (ML) to predict the related risk statements on the risk records. The Predictive Intelligence plugin uses the similarity capability in the Predictive Intelligence engine to compare the risk name and description with the risk statements. With this plugin, your organization can reduce the effort that is required to search and identify

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the risk statements to associate with the identified risks. Your organization also gets higher accuracy in risk aggregation and reporting and visibility into the organization's risk profile.

The following example shows the recommended risk statements on the risk record.




**Note:** A risk user (sn_risk.user) can only see the risk statement recommendations when the risk statement isn't defined on the risk record. Based on the recommendations, a risk user can associate the risk with a related risk statement.

## Benefits of risk categorization with risk statements

By categorizing your organization's risks with the risk statement, the following benefits are provided to different users:

- Risk owners: Identify the correct risk statement for the orphan risks to group risks into manageable categories.
- Risk managers: Reduce the number of orphan risks that were created by the first line of employees or risk champions. The risk managers get visibility into the organization's risk profile and can analyze the impact due to the similar type of risks.
- Risk administrator: Configure the solution definition to predict the risk statements that are based on the organizational needs.

## Setting up the feature

A risk administrator with the ml_admin role can set up the risk categorization in the Risk Workspace application. Before your organization can use this feature, the risk administrator must install and activate the following applications and plugins:

- Risk Management
- Risk Workspace
- Predictive Intelligence
- Recommended Actions - Advanced

A risk administrator can train a default similarity solution for the risks in your organization by using the Predictive Intelligence plugin.

**Note:** A similarity solution is a machine-learning solution to collect and compare your existing records to new similar records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For more information, see Create and train a similarity solution.

**Note:** You must have at least 1000 risk records for the similarity algorithm to work.

A risk administrator with the ml_admin role can review the default similarity solution definition for risk and modify it based on your organizational needs.

## Analyze a risk event in the Risk Workspace

Analyze user-submitted risk events. You can add additional details to the risk event, request more information from the submitter, or reject the risk event if the event is not valid.

### Before you begin

Role required: sn_risk.manager

### About this task

When you a risk event is submitted, it contains basic or little information. As a risk manager, you must add additional details to it when the event is in the **Analyze** state. These additional details consist of the following:

- Approvers of the risk event.
- Root cause of the event.
- Preventative and remedial action for the event.
- Additional entries for the event to break up the event losses.
- Citations
- Tasks
- Impacted controls
- Issues

If you need more information about the risk event, you can ask the submitter to provide you additional information. If you think that the event does not merit attention or is invalid, then you can reject the event.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Risk events** > **All events**.
2. Open the event to analyze and click **Analyze**.
3. Click the Details related list and modify any information that you may need.
   If the risk event occurred but the losses were quickly recovered, the**Full rapid recovery** option is selected. If the risk event resulted in a gain, instead of a loss, the **Financial gain** option is selected. To understand how a risk event can result in a gain, see Manage risk events
4. Click **Save**
5. At this stage, you can do one of the following.

| Task | Action |
|---|---|
| Request approval from the approvers identified. | Click **Request approval**. |
| If further details are required from the submitter, request more information. | Click **Request more information**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Task | Action |
| --- | --- |
| If the risk event is not valid, reject the event. | Click **Reject**. |

6. To add more information to the risk event, click the appropriate related list and add the necessary details.

### What to do next
If the risk event is of subtype **Actual**, create risk event entries. For more information see Create a risk event entry in the Risk Workspace.

## Create a risk event entry in the Risk Workspace

Create a risk event entry to determine the monetary or non-monetary impact of the risk event. A risk event can have multiple risk event entries.

### Before you begin
Role required: sn_risk.manager

### About this task
Risk event entries capture the direct and indirect losses reported due to the risk event. For example, if a risk event of a fire outbreak in an organization is reported, the direct and indirect losses associated with it could be replacing furniture, replacing hardware, losing important data and so on. All these associated losses must be captured individually. You can add risk event entries only for actual events. Potential Risk event entries cannot have risk event entries. You can select any currency while reporting the losses and the currency conversion system will convert the currency to USD.

### Procedure
1. Navigate to **All** > **Risk** > **Risk Workspace** > **Risk events** > **All events**.
2. Open the event for which you want to add risk event entries.
3. Click the Risk Event Entries related list.
4. To create direct and indirect losses, new loss recovery, new additional cost, or new non-financial impact, perform the following actions as necessary.

| To create... | Action |
| --- | --- |
| New direct/indirect loss. | Click **New direct/indirect loss** and fill in the details. |
| New loss recovery | From the **New direct/indirect loss** list, select **New loss recovery** and fill in the details. New loss recovery is amount recovered from the total financial impact. If the amount is recovered within the number of days specified in your configuration, the **Full rapid recovery**option is automatically selected. |
| New additional cost | From the **New direct/indirect loss** list, select **New additional cost** and fill in the details. New additional cost is the cost incurred due to the impact. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

5. Click **Save** and refresh the page.
   The loss amounts get updated on the page.

## Create an ORX external event

Create an Operational Riskdata eXchange (ORX) external risk event to share the risk event of your company with other organizations. This exchange of risk events information acts as a learning for other organizations in the industry and prevents them from making the same errors.

### Before you begin

Role required: sn_risk_workspace.operational_risk_manager

### About this task

The ORX association enables operational and non-financial risk professionals to collect, measure and analyse data in an effective way that is consistent with industry. To view and create an ORX event, you must enable the *Show ORX External Events* property.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **External risk events** > **ORX events**.
2. Click **New**.
3. On the form, fill in the fields.

**New ORX external event form**

| Field | Description |
|---|---|
| Name | Name of the risk event |
| Description | Brief description of the event. |
| Company details | |
| Company | Company in which the event occurred. |
| Region | Region in which the event occurred. |
| Role of the firm | Role the firm had in relation to the transaction. |
| Business line level 2 | Business line of the event. |
| Country | Country in which the event occurred. |
| Counterparty | Type of counterparty or claimant that is involved in the event. |
| ORX member | Option to show if the company is an existing ORX member. |
| Loss details | |
| Loss event id | ID of the loss event. |
| Loss category | Category of the loss. |
| Event type level 2 | Level 2 of the event such as corporate finance, merchant banking and so on. |
| Process code | Code of the process. |
| Product code | Code of the product. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Open | Option to denote if the risk event is open. |
| Sources | Source of the event. |
| Classification | |
| Boundary risk | Operational risk event which triggers a consequence for example, financial loss in another risk category. |
| AMA status | Advanced measurement approach (AMA) is one of three possible operational risk methods that can be used under Basel II by a bank or other financial institution. |
| Financial amounts | |
| Gross loss amount | Gross loss amount. |
| Direct recovery | Any payment other than an indirect recovery received by the firm which offsets the loss. |
| Indirect recovery | Recovery made through insurance. |
| Net Loss (in Local Currency) | Net loss incurred in the local currency. |
| Net Loss (in Euro) | Net loss incurred converted to Euros. |
| Key dates | |
| Date of discovery | Date the event was discovered. |
| Date of event start | Date the event started |
| Date of settlement | Date the event was settled. |
| Date of publication | Date the even was published. |
| Date of event finish | Date the event finished. |
| Cause | |
| Cause level 3 | Third cause level of the event. |
| Additional details | |
| Jurisdiction | Jurisdiction of the event. |
| Scenario category | Category of the scenario such as conduct, external fraud, technology and so on. |
| Environmental volatility | Aspect of the environment or circumstances in which the bank was operating at the time of the event. |
| Activity | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Work notes | Notes that are visible to any responder to this event, their manager, or an administrator. |
| Additional comments | Additional comments about this event. |

## Report a risk event from the Risk Portal

Report a risk event from the Risk Portal. The Risk Portal provides an easy method to quickly report risk events.

### Before you begin

Role required: sn_grc.business_user role

### Procedure

1. Navigate to **Risk Portal**.
2. Under Report, click **Risk event**
   The Report Risk Event form is displayed.
3. On the form, fill in the fields.
4. Click **Submit for review**.

### Result

The risk event is created and submitted for the risk team's review.

## Chart colors for risk data

You can view your risk data visualizations in different colors for a quick overview of your risks.

Various risk reports appear on the Risk home page. Some examples of these reports are pie charts, bar graphs and so on. These reports show the risk ratings in different colors. By default, ServiceNow® provides the chart colors for the following risk ratings for Advanced Risk Assessments.

- Very high
- Critical
- Ineffective
- High
- Medium
- Moderate
- Needs improvement
- Low
- Effective
- Very low

For classic risk, the following risk criteria are defined with the respective colors:

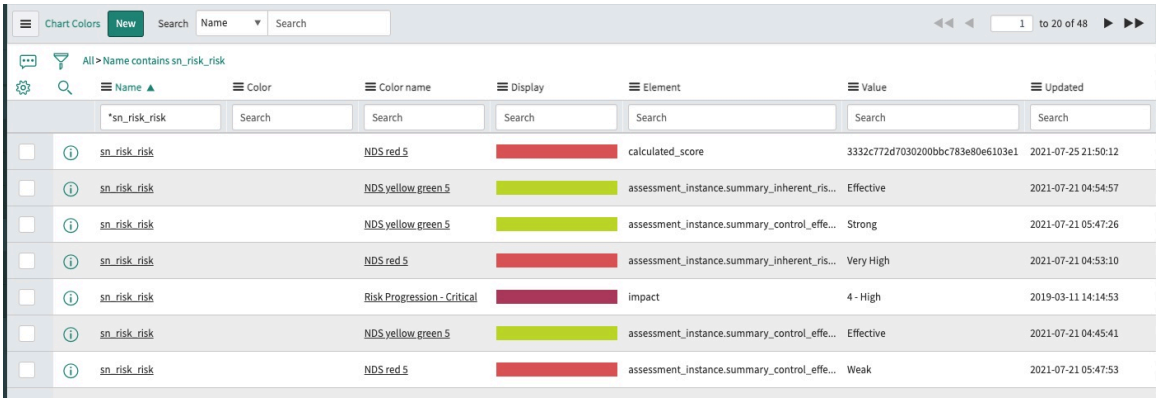
- Very low
- Low
- Moderate

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- High
- Very high

If you want to add or modify a risk criteria or a risk rating, a report administrator with the role, report_admin, can configure your chart colors. For more information on configuring chart colors, see Using chart colors.

**Chart colors**




## Create a business process in the Risk Workspace

Create a business process in the Risk Workspace and define the owners, approvers, business criticality, and review frequency for the process.

### Before you begin

Role required: Enterprise architect or service owner or itil

### About this task

When you create a business process, it is important to ascertain the CIA triad. CIA triad refers to confidentiality, integrity, and availability. The CIA triad is a common model that forms the basis for the development of security systems and policies. These are used for the identification of vulnerabilities and methods for addressing problems and creating solutions.

### Procedure

1. Navigate to **All** > **Risk Workspace** > **Lists** > **Business Processes**.
2. Click **Create New**.
3. On the form, fill in the fields.

**Business Process form**

| Field | Description |
|---|---|
| Name | Name of the business process. |
| Description | Description of the business process. |
| Parent | Parent business process, if it exists, to create a hierarchy of business processes. |
| Review frequency | Frequency for reviewing the business process. |
| Ownership | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Life cycle stage | Stage of record in the business life cycle. The stage determines the status and displays the actions. This field is automatically set to **Ideation** when you save the form for a process in **Draft** state. |
| Managed by group | Group that maintains the business process. |
| Approval group | Group that must review and approve the business process. |
| Owned by | User responsible for the business process. This user is a member of the Managed by group. |
| Life cycle stage status | Status of business process within the life cycle stage. This field is automatically set to **Under Evaluation** when you save the form for a process in **Draft** state. |
| Next review date | Planned date on which the business process must be reviewed. The value in this field is automatically set only after the business process is approved. |
| Description | Short description of the business process. The description can include the background, the actual steps, and the interaction of the process. |
| Business Impact | |
| Business criticality declared | Criticality of the business process based on your subjective assessment. The choices are:<br>◦ **1- most critical**<br>◦ **2- somewhat critical**<br>◦ **3- less critical**<br>◦ **4- not critical** |
| Business criticality determined | Computed criticality of the business process based on the assessment of the sub-processes. The choices are:<br>◦ **1- most critical**<br>◦ **2- somewhat critical**<br>◦ **3- less critical**<br>◦ **4- not critical** |
| CIA triad | |
| Impact to confidentiality | Risk rating for the risk of loss of confidentiality for the process. The choices are:<br>◦ **High**<br>◦ **Medium**<br>◦ **Low** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Impact to integrity | Risk rating for the risk of impact to integrity for the process. The choices are:<br>◦ **High**<br>◦ **Medium**<br>◦ **Low** |
| Impact to availability | Risk rating for the risk of loss of availability for the process. The choices are:<br>◦ **High**<br>◦ **Medium**<br>◦ **Low** |

4. Right-click and save the form.
   The record moves to the **Draft** state.

Related topics

Add related assets to a business process

### Add related assets to a business process

Add related business assets to a business process to gain visibility into the IT assets and their performance.

#### Before you begin
Role required: Enterprise architect or service owner or itil

#### About this task
A business process is supported by various assets such as business applications, network servers, application servers and their services and so on. It is important that a process owner is able to establish that relationship and then have visibility into these IT assets and their performance. For example, assume that employee leave management is a business process. This business process depends on an application to automate it. The application, in turn, depends on servers to run it. Thus, if you relate the assets to a process, you can track the overall performance of your processes.

#### Procedure
1. Navigate to **All** > **Risk Workspace** > **Lists** > **Business Processes**.
2. Open the business process to which you want to add assets and click the Related assets related list.
3. Click **Add**.
   The Related Assets pop up appears.
4. Select the related assets you want to add to the business process.
5. Click **Add**.
6. Click **Save**.

## Create a test plan in Risk Workspace

Create a test plan to document the control testing procedure. You can create a test plan from scratch or based on a test template to describe how a feature is to be tested.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Before you begin**
Role required: admin

**Procedure**

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Control testing** > **Control test plans**.
2. Click **New**.
3. On the form, fill in the fields.

**Create New Test plan form**

| Field | Description |
|---|---|
| Number | Unique identification number. |
| Name | Name of the test plan. |
| Control | The control that this test plan covers. |
| Entity | Entity is auto-populated based on the value selected in the **Control** field. |
| Test template | Related test template.<br><br>If you select a test template, all the fields in the **Design test** and **Operational test** sections are populated with the test template values. |
| Duration | Expected duration of the test. |
| Design test | |
| Design expectations | Basic requirement that should be met for a control to be effective. |
| Design assessment procedures | Procedure or steps to be followed to conclude whether the design of the control is effective to achieve the control objective or not. This is based on the design expectation. |
| Operational test | |
| Operational expectations | Expectations that should be met to ensure that the control is operating effectively to achieve the control objective. |
| Operational assessment procedures | Detailed steps, to carry out the operational expectations, which need to be performed to conclude that the control is operating successfully. |

4. Click **Save**.
5. To visually explore the relationships between the different types of critical audit data that affect your business, click **360° view** button.

## Filter data in the risk heatmap workbench

As a risk user, filter data in the risk heatmap workbench to get a granular view of your risks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_risk_workspace.operational_risk_manager, sn_risk_workspace.business_op_risk_manager

### About this task
Using the condition builder feature, the risk heatmap workbench enables you to further filter the risks that need your attention. For example, you can filter risks with high rating. If you have an important filter that you use frequently, you can also save the filter.

### Procedure
1. Navigate to **All** > **Risk Management** > **Risk Workspace**.
2. From the Home page, select the launch workbench icon ( ).
3. Select Filter.
4. In the Advanced view dialog box, provide the values for field, operator, and value.
5. Select **Submit**.
   The heatmap is refreshed with the filtered results.
6. To view the filter conditions that you have built and applied, select **Filter Overview**.
7. To clear the filter condition results, select **Clear results**.
8. To save the filter, select the save filter button ( ) in the Contextual side panel.
   a. In the **Title** field, provide a title for the filter.
   b. Select **Save**.
   The saved filter appears in the My saved filters related list.
9. To delete a filter condition that you have built, open the Filter dialog box, and select the delete condition button ( ) and click **Submit**.

## Define the risk appetite for an entity

Define the risk appetite on the entity records in the Risk Management application to evaluate all the possible risks and to set the boundaries for the acceptable and unacceptable risks for your business.

### Before you begin
Role required: sn_risk.user

### About this task
Entity owners can define the risk appetite and tolerance and then copy the qualitative risk appetite to the downstream entities. By doing this task, a business can define and manage an action plan when there's a breach. By defining the qualitative (numerical scale and ratings) and quantitative (monetary value) appetite, a risk user can understand the risk appetite and take decisions. For more information on the risk appetite and tolerance, see Risk appetite and tolerance in Advanced Risk.

### Procedure
1. Navigate to **All** > **Risk** > **Risk Workspace**.
2. Select the list icon and navigate to the entity.
3. Define the risk appetite for a new or an existing entity:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- To define the risk appetite for a new entity, select **New**.
- To define the risk appetite for an existing entity, select and open the required entity record.

4. On the entity form, select the **Risk Appetite** section and fill in the fields.

   For a description of the field values, see Risk appetite fields on the Entity form.

5. Select **Save**.
6. Optional: To copy the qualitative appetite to the downstream entities, select the more actions icon on the form and select **Copy qualitative appetite**.

> **Important:** You can only copy the qualitative appetite and tolerance to downstream entities when the risk appetite of the downstream entity isn't overridden. You must define the quantitative appetite and tolerance for each level in the hierarchy.

### Risk appetite fields on the Entity form

Learn about the risk appetite fields on the Entity form. Use these fields to define the risk appetite, evaluate all the possible risks, and set the boundaries for the acceptable and unacceptable risks in the Risk Management application.

See the following table for a description of the field values.

> **Note:** The risk appetite fields that appear on the entity form depends on the advanced risk assessment properties set by the risk administrator.

**Risk appetite fields on the Entity form**

| Field | Description |
|---|---|
| Override qualitative risk appetite | Option to override the qualitative risk appetite of the parent entity. By default, all entities inherit the risk appetite of the upstream entity in the entity form. When you select this option, you can define the risk appetite values for the current entity separately.<br>**Note:** This field appears only when there's an upstream entity available for the current entity. |
| Qualitative appetite | Risk appetite in numerical scale and rating terms. The qualitative appetite is compared with the qualitative risk rating to compute the qualitative appetite status. You can define the qualitative appetite based on the appetite scale set by the risk administrator. The default options are as follows:<br>• 1 - Averse<br>• 2 - Minimalist<br>• 3 - Cautious |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Entity form (continued)**

| Field | Description |
| --- | --- |
| | • 4 - Open<br>• 5 - Hungry<br><br>A risk administrator can change or create the risk appetite scales based on the organization's requirement. For more information, see Set up a risk appetite scale.<br><br>After you define the qualitative appetite, you can copy it to the downstream entities.<br><br>**Note:** A risk user and risk reader with the sn_risk_advanced.qualitative_risk_appetite_reader role can only view the qualitative appetite and qualitative tolerance values on the form and in other places. |
| Quantitative appetite | Risk appetite in quantitative terms. The quantitative risk appetite can be measured and expressed in monetary values. The quantitative appetite is the amount of loss that an organization is willing to risk. For example, an organization decides to have $10,000 (US dollars) as a target non-performing asset (NPA) for this year, which means that the organization defines $10,000 (US dollars) as the quantitative risk appetite.<br><br>The quantitative appetite is compared with the annual loss expectancy (ALE) to compute the quantitative appetite status.<br><br>**Note:** A risk user and risk reader with the sn_risk_advanced.quantitative_risk_appetite_reader role can only view the quantitative appetite and the quantitative tolerance values on the form and in other places. |
| Qualitative tolerance | Risk tolerance in numerical scale and rating terms. The risk tolerance is the standard deviation from the defined risk appetite. The qualitative tolerance is compared with the qualitative risk rating to compute the qualitative appetite status. The qualitative tolerance should be greater than the defined qualitative appetite. You can define the qualitative tolerance based on the appetite scale that is set by the risk |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Entity form (continued)**

| Field | Description |
|---|---|
| | administrator. The default options are as follows:<br>• 1 - Averse<br>• 2 - Minimalist<br>• 3 - Cautious<br>• 4 - Open<br>• 5 - Hungry<br><br>A risk administrator can modify or create the risk appetite scales based on the organization's requirement. For more information, see Set up a risk appetite scale. |
| Quantitative tolerance | Risk tolerance in quantitative terms. The risk tolerance is the standard deviation from the defined risk appetite. The quantitative risk tolerance can be measured and expressed in monetary values. For example, an organization decides to have $15,000 (US dollars) as a target non-performing asset (NPA) for this year, which means that the organization defines $15,000 as the quantitative risk tolerance.<br><br>The quantitative tolerance is compared with the annual loss expectancy (ALE) to compute the quantitative appetite status.<br><br>**Note:** The quantitative tolerance should be greater than the defined quantitative appetite. |
| Risk appetite status | |
| Qualitative appetite status | Qualitative appetite status of the entity. The qualitative appetite status is calculated by comparing the defined qualitative appetite with the qualitative appetite that is mapped to the final risk rating. A risk administrator can map the appetite scales to the risk rating criteria for the final assessment type in the risk assessment methodology (RAM).<br><br>**Note:** The primary RAM that is associated with the entity class is considered for status calculation.<br><br>For example, if you define the qualitative appetite as 2-Minimalist and the qualitative tolerance as 4-Open, then the following statuses appear: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Entity form (continued)**

| Field | Description |
|---|---|
| | • For a qualitative risk rating of 1- Averse or 2-Minimalist, the appetite status is within appetite.<br>• For a qualitative risk rating of 3-Cautious or 4-Open, the appetite status is outside the appetite.<br>• For a qualitative risk rating of 5-Hungry, the appetite status is outside the tolerance. |
| Quantitative appetite status | Quantitative appetite status of the entity. The annual loss expectancy (ALE) values are compared with the defined quantitative appetite to calculate this appetite status.<br>**Note:** The aggregated ALE value from the primary RAM that is associated with the entity class are considered for the status calculation.<br>For example, if you define the quantitative appetite as $1000 (US dollars) and the quantitative tolerance as $1500, then the following statuses appear:<br>• For ALE equal to or less than $1000, the appetite status is within the appetite.<br>• For ALE ranges from $1001 to $1500, the appetite status is outside the appetite.<br>• For ALE more than $1500, the appetite status is outside the tolerance. |
| Appetite status | Overall appetite status. The overall appetite status considers the worst-case scenario between the qualitative and quantitative status. For example, if the qualitative appetite status is within the appetite and the quantitative appetite status is outside the appetite, then the overall appetite status is outside the appetite. |

## Define the risk appetite for a risk

Define the risk appetite on the risk records in the Risk Management application to evaluate all possible risks and to set the boundaries for acceptable and unacceptable risks.

### Before you begin

Role required: sn_risk.user

### About this task

Risks inherit the appetite value from the associated risk statement. Risk owners can also define the risk appetite and tolerance on the risk form when there's a business requirement to

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

override the parent value. For more information on the risk appetite and tolerance, see Risk appetite and tolerance in Advanced Risk.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace**.
2. Select the list icon and navigate to the risk.
3. Define the risk appetite for a new or an existing risk:
   - To define the risk appetite for a new risk, select **New**.
   - To define the risk appetite for an existing risk, select and open the required risk record.
4. On the risk form, select the **Risk Appetite** section and fill in the fields.

   For a description of the field values, see Risk appetite fields on the Risk form.
5. Select **Save**.

#### Risk appetite fields on the Risk form

Learn about the risk appetite fields on the Risk form. Use these fields to define the risk appetite, evaluate all the possible risks, and set the boundaries for acceptable and unacceptable risks in the Risk Management application.

See the following table for a description of the field values.

**Note:** The risk appetite fields that appear on the entity form depends on the advanced risk assessment properties set by the risk administrator.

#### Risk appetite fields on the Risk form

| Field | Description |
|---|---|
| Override qualitative risk appetite | Option to override the qualitative risk appetite of the risk statement. By default, all risks inherit the risk appetite of the risk statement in the risk form. When you select this option, you can define the risk appetite values for the current risk separately.<br>**Note:** This field appears only when there's an associated risk statement available for the current risk. |
| Justification for override | Reason to override the qualitative risk appetite values of the risk statement in the current risk. This information helps the risk manager to understand the business need for the override.<br>**Note:** This field appears only when the **Override qualitative risk appetite** option is selected. |
| Qualitative appetite | Risk appetite in numerical scale and rating terms. The qualitative appetite is compared |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Risk form (continued)**

| Field | Description |
| --- | --- |
| | with the qualitative risk rating to compute the qualitative appetite status. You can define the qualitative appetite based on the appetite scale set by the risk administrator. The default options are as follows:<br>• 1 - Averse<br>• 2 - Minimalist<br>• 3 - Cautious<br>• 4 - Open<br>• 5 - Hungry<br><br>A risk administrator can change or create the risk appetite scales based on the organization's requirement. For more information, see Set up a risk appetite scale.<br><br>**Note:** A risk user and risk reader with the sn_risk_advanced.qualitative_risk_appetite_reader role can only view the qualitative appetite and qualitative tolerance values on the form and in other places. |
| Quantitative appetite | Risk appetite in quantitative terms. The quantitative risk appetite can be measured and expressed in monetary values. The quantitative appetite is the amount of loss that an organization is willing to risk. For example, an organization decides to have $10,000 (US dollars) as the target non-performing asset (NPA) for this year, which means that the organization defines $10,000 (US dollars) as the quantitative risk appetite.<br><br>The quantitative appetite is compared with the annual loss expectancy (ALE) to compute the quantitative appetite status.<br><br>**Note:** A risk user and risk reader with the sn_risk_advanced.quantitative_risk_appetite_reader role can only view the quantitative appetite and quantitative tolerance values on the form and in other places. |
| Qualitative tolerance | Risk tolerance in numerical scale and rating terms. The risk tolerance is the standard deviation from the defined risk appetite. The qualitative tolerance is compared with the qualitative risk rating to compute the |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Risk form (continued)**

| Field | Description |
| --- | --- |
| | qualitative appetite status. The qualitative tolerance should be greater than the defined qualitative appetite. You can define the qualitative tolerance based on the appetite scale set by the risk administrator. The default options are as follows:<br>• 1 - Averse<br>• 2 - Minimalist<br>• 3 - Cautious<br>• 4 - Open<br>• 5 - Hungry<br><br>A risk administrator can change or create the risk appetite scales based on the organization's requirement. For more information, see Set up a risk appetite scale. |
| Quantitative tolerance | Risk tolerance in quantitative terms. The risk tolerance is the standard deviation from the defined risk appetite. The quantitative risk tolerance can be measured and expressed in monetary values. For example, an organization decides to have $15,000 (US dollars) as a target non-performing asset (NPA) for this year, which means that the organization defines $15,000 (US dollars) as the quantitative risk tolerance.<br><br>The quantitative tolerance is compared with the annual loss expectancy (ALE) to compute the quantitative appetite status.<br><br>**Note:** The quantitative tolerance should be greater than the defined quantitative appetite. |
| Risk appetite statement | Risk appetite statement that defines the amount and types of risk an organization is willing to accept to achieve its objectives. It documents what the organization considers as threats and its response strategies. These statements give additional context to understand the risk appetite and help the business to make risk-informed decisions. For example, `"ACME Inc. has no appetite for unauthorized access to systems and confidential data and will maintain strong controls to mitigate external threats against its technology infrastructure.` |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Risk form (continued)**

| Field | Description |
|---|---|
| | ACME Inc. has a low appetite for losing the continuity of business operations stemming from unreliable telecommunications or system availability. Business resiliency planning and execution must be aligned with strategic objectives. ACME Inc. has a moderate appetite for innovative technology solutions to meet user demands in a rapidly changing environment. The agency will exercise appropriate governance and discipline when considering and adopting new technology." |
| Risk appetite status | |
| Qualitative appetite status | Qualitative appetite status of the risk. The qualitative appetite status is calculated by comparing the defined qualitative appetite with the qualitative appetite that is mapped to the final risk rating. A risk administrator can map the appetite scales to the risk rating criteria for the final assessment type in the Risk assessment methodology (RAM).<br><br>**Note:** The primary RAM that is defined in the associated entity is considered for status calculation.<br><br>For example, if you define the qualitative appetite as 2-Minimalist and the qualitative tolerance as 4-Open, then the following statuses appear:<br>• For a qualitative risk rating of 1- Averse or 2-Minimalist, the appetite status is within the appetite.<br>• For a qualitative risk rating of 3-Cautious or 4-Open, the appetite status is outside the appetite.<br>• For a qualitative risk rating of 5-Hungry, the appetite status is outside the tolerance. |
| Quantitative appetite status | Quantitative appetite status of the risk. The annual loss expectancy (ALE) values are compared with the defined quantitative appetite to calculate this appetite status.<br><br>**Note:** The risk assessment ALE value from the primary RAM that is defined in the associated entity are considered for status calculation. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Risk form (continued)**

| Field | Description |
|---|---|
| | For example, if you define the quantitative appetite as $1000 (US dollars) and the quantitative tolerance as $1500 (US dollars), then the following statuses appear:<br>• For ALE that is equal to or less than $1000 (US dollars), the appetite status is within the appetite.<br>• For ALE ranges from $1001 to $1500 (US dollars), the appetite status is outside the appetite.<br>• For ALE more than $1500 (US dollars), the appetite status is outside the tolerance. |
| Appetite status | Overall appetite status. The overall appetite status considers the worst-case scenario between the qualitative and quantitative status. For example, if the qualitative appetite status is within the appetite and the quantitative appetite status is outside the appetite, then the overall appetite status is outside the appetite. |

## Define the risk appetite for a risk statement

Define the risk appetite on the risk statement records in the Risk Management application to evaluate all the possible risks and set the boundaries for the acceptable and unacceptable risks.

### Before you begin

Role required: sn_risk.manager

### About this task

A risk manager can define the risk appetite and tolerance for the risk statement and then copy the qualitative risk appetite to the downstream risk statements and risks. It helps businesses to take risks within their organizational capabilities and define and manage an action plan when there's a breach. By defining the qualitative (numerical scale and ratings) and quantitative (monetary value) appetite, a risk user can understand the risk appetite and take decisions. For more information on the risk appetite and tolerance, see Risk appetite and tolerance in Advanced Risk.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace**.
2. Select the list icon and navigate to the risk statement.
3. Define the risk appetite for a new or an existing risk statement:
   - To define the risk appetite for a new risk statement, select **New**.
   - To define the risk appetite for an existing risk statement, select and open the required risk statement record.
4. On the form, select the **Risk Appetite** section and fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For a description of the field values, see Risk appetite fields on the Risk Statement form.

5. Select **Save**.
6. Optional: To copy the qualitative appetite to the downstream risk statement and risks, select the more actions icon on the form and select **Copy qualitative appetite**.

**Important:** You can only copy the qualitative appetite and tolerance to the downstream risks and risk statements when the risk appetite isn't overridden. You need to define quantitative appetite and tolerance for each level in the hierarchy.

### Risk appetite fields on the Risk Statement form

Learn about the risk appetite fields on the Risk Statement form. Use these fields to define the risk appetite, evaluate all the possible risks, and set the boundaries for the acceptable and unacceptable risks in the Risk Management application.

See the following table for a description of the field values.

**Note:** The risk appetite fields that appear on the entity form depends on the advanced risk assessment properties that are set by the risk administrator.

#### Risk appetite fields on the Risk Statement form

| Field | Description |
|---|---|
| Override qualitative risk appetite | Option to override the qualitative risk appetite of the parent risk statement. By default, all risk statements inherit the risk appetite of the parent risk statement. When you select this option, you can define the risk appetite values for the current risk statement separately.<br><br>**Note:** This field appears only when there's a parent risk statement available for the current risk statement. |
| Qualitative appetite | Risk appetite in numerical scale and rating terms. The qualitative appetite is compared with the qualitative risk rating to compute the qualitative appetite status. You can define the qualitative appetite based on the appetite scale that is set by the risk administrator. The default options are as follows:<br>• 1 - Averse<br>• 2 - Minimalist<br>• 3 - Cautious<br>• 4 - Open<br>• 5 - Hungry<br><br>A risk administrator can change or create the risk appetite scales based on the |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Risk Statement form (continued)**

| Field | Description |
|---|---|
| | organization's requirement. For more information, see Set up a risk appetite scale.<br><br>After you define the qualitative appetite, you can copy it to the downstream risks and risk statements.<br><br>**Note:** A risk manager with the sn_risk_advanced.qualitative_risk_appetite_reader role can only view the qualitative appetite and qualitative tolerance values on the form and in other places. |
| Quantitative appetite | Risk appetite in quantitative terms. The quantitative risk appetite can be measured and expressed in monetary values. The Quantitative appetite is the amount of loss that an organization is willing to risk. For example, an organization decides to have $10,000 (US dollars) as a target non-performing asset (NPA) for this year, which means that the organization defines $10,000 (US dollars) as the quantitative risk appetite.<br><br>The quantitative appetite is compared with the annual loss expectancy (ALE) to compute the quantitative appetite status.<br><br>**Note:** A risk manager with the sn_risk_advanced.quantitative_risk_appetite_reader role can only view the quantitative appetite and quantitative tolerance values on the form and in other places. |
| Qualitative tolerance | Risk tolerance in numerical scale and rating terms. The risk tolerance is the standard deviation from the defined risk appetite. The qualitative tolerance is compared with the qualitative risk rating to compute the qualitative appetite status. The qualitative tolerance should be greater than the defined qualitative appetite. You can define the qualitative tolerance based on the appetite scale set by the risk administrator. The default options are as follows:<br>• 1 - Averse<br>• 2 - Minimalist<br>• 3 - Cautious<br>• 4 - Open<br>• 5 - Hungry |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Risk Statement form (continued)**

| Field | Description |
|---|---|
| | A risk administrator can change or create the risk appetite scales based on the organization's requirement. For more information, see Set up a risk appetite scale. |
| Quantitative tolerance | Risk tolerance in quantitative terms. The risk tolerance is the standard deviation from the defined risk appetite. The quantitative risk tolerance can be measured and expressed in monetary values. For example, an organization decides to have $15,000 (US dollars) as the target non-performing assets (NPAs) for this year. This means that the organization defines $15000 (US dollars) as the quantitative risk tolerance.<br><br>The quantitative tolerance is compared with the annual loss expectancy (ALE) to compute the quantitative appetite status.<br><br>**Note:** The quantitative tolerance should be greater than the defined quantitative appetite. |
| Risk appetite statement | Risk appetite statement that defines the amount and types of risk that an organization is willing to accept to achieve its objectives. It documents what the organization considers threats and its response strategies. These statements give additional context to understand the risk appetite and help the business to make risk-informed decisions. For example, `"ACME Inc. has no appetite for unauthorized access to systems and confidential data and will maintain strong controls to mitigate external threats against its technology infrastructure. ACME Inc. has a low appetite for losing the continuity of business operations stemming from unreliable telecommunications or system availability. Business resiliency planning and execution must be aligned with strategic objectives. ACME Inc. has a moderate appetite for innovative technology solutions to meet user demands in a rapidly changing environment. The agency will exercise appropriate governance and discipline when` |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Risk Statement form (continued)**

| Field | Description |
|---|---|
| | considering and adopting new technology." |
| Next review date | Date to update the risk appetite fields and review the risk appetite statement. An email notification is sent to the risk statement owner before the next review date. A risk administrator can schedule the email notification in the advanced risk assessment properties. For more information, see Configure a risk appetite and tolerance in Advanced Risk. |
| Risk appetite status | |
| Methodology for status calculation | Risk assessment methodology (RAM) whose aggregated results are used to calculate the risk appetite status of the risk statement. |
| Qualitative appetite status | Qualitative appetite status of the risk statement. The qualitative appetite status is calculated by comparing the defined qualitative appetite with the qualitative appetite that is mapped to the final risk rating. A risk administrator can map the appetite scales to the risk rating criteria for the final assessment type in RAM.<br>**Note:** The RAM selected from the **Methodology for status calculation** field is considered for the status calculation.<br>For example, if you define the qualitative appetite as 2-Minimalist and qualitative tolerance as 4-Open, then the following statuses appear:<br>• For a qualitative risk rating of 1- Averse or 2-Minimalist, the appetite status is within appetite.<br>• For a qualitative risk rating of 3-Cautious or 4-Open, the appetite status is outside appetite.<br>• For a qualitative risk rating of 5-Hungry, the appetite status is outside the tolerance. |
| Quantitative appetite status | Quantitative appetite status of the risk statement. The annual loss expectancy (ALE) values are compared with the defined quantitative appetite to calculate this appetite status. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk appetite fields on the Risk Statement form (continued)**

| Field | Description |
|---|---|
| | **Note:** The aggregated ALE value from the RAM that are selected from the **Methodology for status calculation** field are considered for the status calculation.<br><br>For example, if you define the quantitative appetite as $1000 (US dollars) and the quantitative tolerance as $1500 (US dollars), then the following statuses appear:<br>• For ALE equal to or less than $1000, the appetite status is within appetite.<br>• For ALE ranges from $1001 to $1500, the appetite status is outside the appetite.<br>• For ALE more than $1500, the appetite status is outside the tolerance. |
| Appetite status | Overall appetite status. The overall appetite status considers the worst-case scenario between the qualitative and quantitative status. For example, if the qualitative appetite status is within the appetite and the quantitative appetite status is outside the appetite, then the overall appetite status is outside the appetite. |

## Parallel Review and Feedback in Advanced Risk

Learn how to use the Review and feedback workflow to enable the 2nd and 3rd line managers to review records, capture feedback, and track the closure of feedback.

## Overview

The Parallel Review and Feedback in the Advanced Risk application helps in collaboration and engagement across different lines of management within an organization. The workflow enables the 2nd and 3rd line managers, such as Operational, IT, and Business Risk Managers, to provide feedback on records or fields in the records. For example, a risk manager can provide feedback by requesting a root cause analysis at the field level of the risk event. Alternatively, they may request the risk event owner to provide details of additional loss entries at the record level for the same risk event. Risk managers can create feedback on records available on the ServiceNow table and external records.

## Benefits of Parallel Review and Feedback

The Parallel Review and Feedback application enables you to do the following:

- Provide feedback at any stage of the workflow.
- Update the feedback responses directly from the source record by using the side-panel feature.
- View and manage the feedback workflows that are raised against the records from a centralized dashboard.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- View the change history, which enables a quick comparison of pre-feedback and post-feedback.
- Reopen the feedback if the responses are deemed unsatisfactory.
- Monitor the feedback and follow up with the record owners through an intuitive dashboard.
- Collaborate effectively with the reviewer, respondent, and other stakeholders through a sidebar discussion chat.
- Initiate and link further actions as outcomes of the feedback, such as creating an issue or linking to an existing one.
- Configure a feedback integration setup for any record type, including custom tables where you can define the table or record type to create feedback from.

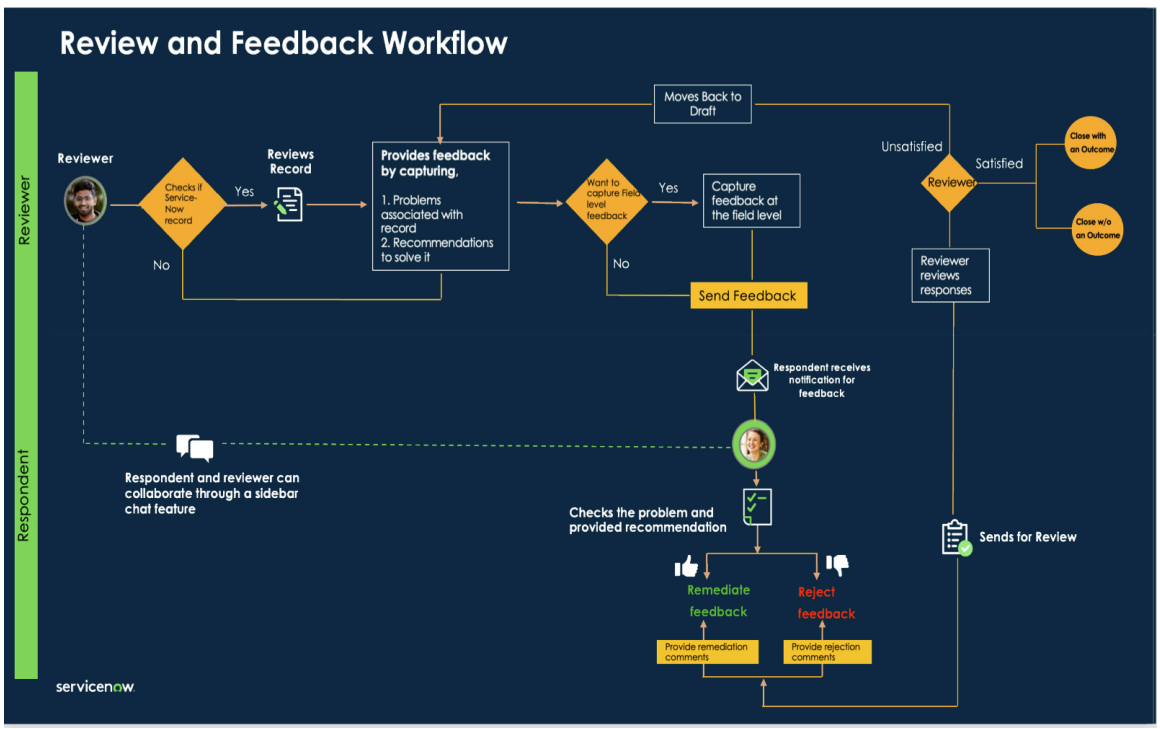
### Parallel Review and Feedback workflow

The Parallel Review and Feedback workflow outlines the systematic process by which the solution facilitates the submission of feedback on a record or specific fields within a record. Feedback could be related to any improvement or recommendation at a record level, such as data integrity, compliance, and operational procedures.

## Exploring the user journey for Parallel Review and Feedback

The following diagram shows the workflow of Review and Feedback.

**Parallel Review and Feedback workflow**




The steps for how each user uses the Review and Feedback application according to their organization's requirements are explained as follows.

Configure a feedback integration

Configure a feedback integration setup in the Advanced Risk application to define the table on which you want to use Parallel Review and Feedback. This setup enables you to define the workspace, reviewer, and respondent for creating feedback on the table records. A user with the sn_rvw_feedback.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

role can configure a feedback integration. For more details, see Configure a feedback integration.

Create the feedback

A user with the sn_rvw_feedback.reviewer role can create feedback on a record they're reviewing, suggesting overall improvements, or changes to specific fields in the record. You can create feedback on both ServiceNow® and external records. For more information, see Create feedback in the Risk Workspace and Create Feedback from the record side panel.

Respond to the feedback

A user with the sn_rvw_feedback.respondent role can take necessary actions and provide comments or explanations regarding the submitted feedback. The respondent can either remediate or reject the feedback, provided that there's proper justification. After closing all the open items, the respondent can send the feedback to the reviewer. For more information, see Respond to the feedback.

Collaborate through sidebar chat feature

The Sidebar chat feature enabling the first and second line risk users to discuss feedback in real-time. The chat feature enables better collaboration among different stakeholders to brainstorm solutions, clarify details, or coordinate actions regarding the feedback received. For more information, see Initiate a chat from Sidebar in Parallel Review and Feedback.

Review and close the feedback

When the reviewer is content with the respondent's comments, they have a couple of options. They can choose to close the feedback either with or without an action. If an action is selected, they can take further actions based on the feedback received. It involves initiating new actions or tasks, such as creating an issue or linking it to an existing record, to facilitate follow-up and resolution. For example, an organization conducted an RCSA (Risk and control self-assessment) concerning fraud-related risks and suggested they have 3 controls in place. Subsequently, the second line of defense reviewed the assessment and raised a feedback, recommending the addition of a new control as it aligns with global best practices to mitigate that risk. Implementing this new control requires budget allocation and an estimated timeline of 1-2 years. The organization may decide to close the feedback by creating an issue to track and manage the progress.

When the reviewer isn't satisfied with the respondent comments, the reviewer can move the feedback to the Draft state and reinitiate the workflow. For more information, see Review and close the feedback.

### Feedback dashboard

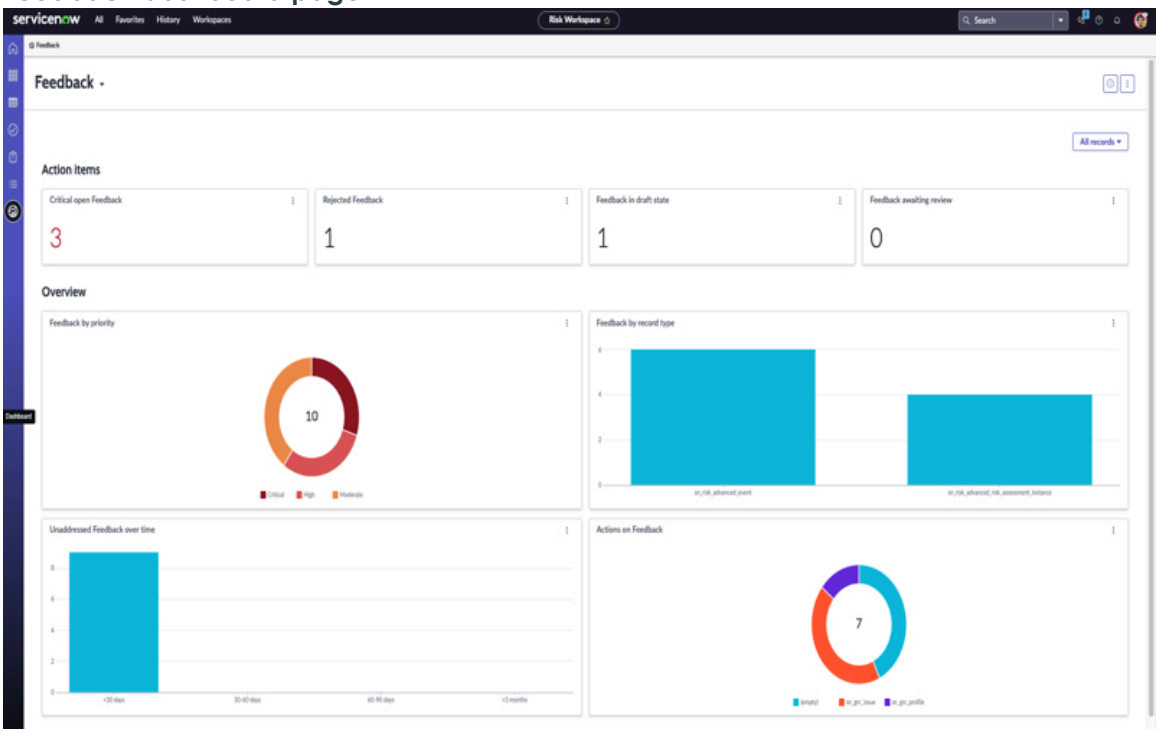
Use the Feedback dashboard to track and manage feedback using the Risk Workspace. The Feedback dashboard organizes feedback according to its status, importance, type, and other specific factors.

## Overview

You can launch the Feedback dashboard by using the launcher  icon. The following example shows the cards that are available on the Feedback dashboard.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Feedback dashboard page




You can analyze and monitor only relevant information by filtering the dashboard based on different record types. You can navigate to **All records** and select the respective record type to visualize related information on the dashboard. The available record types are based on the active feedback configurations.

The following table describes the cards that are available on the Feedback dashboard landing page.

#### Feedback dashboard

| Section | Card | Description |
|---|---|---|
| Action items | Critical open Feedback | Shows the feedback with priority as **Critical**. |
| | Rejected Feedback | Shows the feedback with response as **Rejected**. |
| | Feedback in draft state | Shows the feedback that hasn't yet been sent to the respondent. |
| | Feedback awaiting review | Shows the feedback that hasn't yet been reviewed by the reviewer following the respondent's comments. |
| Overview | Feedback by priority | Shows the active feedback based on their assigned priorities. This helps in understanding the proportion of feedback categorized by urgency levels. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Feedback dashboard (continued)**

| Section | Card | Description |
|---|---|---|
| | Feedback by record type | Shows the feedback based on their record types. This helps in understanding the proportion of feedback categorized by the source records. |
| | Unaddressed Feedback over time | Shows the unaddressed feedback over time. The bar chart displays the trend of unresolved feedback, enabling teams to measure their responsiveness and workload distribution. |
| | Actions on Feedback | Shows the closed feedback with initiated actions and feedback with no actions taken. It facilitates the analysis of what further actions are generally taken as an outcome of the feedback. |

### Configure a feedback integration

Configure a feedback integration setup in the Advanced Risk application to define the table on which you want to use Parallel Review and Feedback. This setup enables you to define the workspace, reviewer, and respondent for creating feedback on the table records.

#### Before you begin

Role required: sn_rvw_feedback.admin

#### Procedure

1. Navigate to **All** > **Parallel Review and Feedback** > **Feedback** > **Administration** > **Feedback Integration Configuration**.
2. Select **New**.
3. On the form, fill in the fields.

   For a description of the field values on the Feedback Integration Configuration form, see Feedback integration configuration form.
4. Select **Submit**.

### Feedback integration configuration form

Use the Feedback integration configuration form to define a setup for the Parallel Review and Feedback.

See the following table for a description of the field values.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Feedback integration configuration form**

| Field | Description |
|---|---|
| Table | Name of the table to integrate review and feedback. For example, if you want to provide feedback on the risk event records, you must select the sn_risk_advanced_event table. |
| Reviewer group | Reviewer group who can provide feedback on the selected table records. |
| Active | State of the feedback integration configuration. Only active configurations can be considered to provide feedback on the selected table records. |
| Workspace URL path | Workspace URL path to send feedback-related notifications to a particular workspace. For example, to use it on the Risk Workspace, select `risk/risk`. |
| Respondent | |
| Respondent type | Respondent who can respond to the raised feedback on the selected table records. The options are as follows:<br>• **User on target record**: Individual who can respond to the feedback.<br>• **Group on target record**: Group of users who can respond to the feedback. |
| Respondent field | User or group field on the target record. For example, if you want the record owner to respond to the raised feedback, select `Owner` in this field. |

### Create feedback in Advanced Risk

Create feedback on a record or fields in a record in the Advanced Risk application. The feedback enables you to recommend improvements related to data integrity, compliance, operational procedures, and other pertinent areas.

You can create feedback by using one of the following options:

- Create feedback in the Risk Workspace
- Create Feedback from the record side panel

### Create feedback in the Risk Workspace

Create feedback on a record or fields in a record, to recommend improvements related to data integrity, compliance, operational procedures, and other pertinent areas, such as disposition and accountability.

**Before you begin**
Role required: sn_rvw_feedback.reviewer

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace**.
2. Select the list  icon.
3. From the list, navigate to **Parallel Review and Feedback** and select **Feedback**.
4. Select **New**.
5. On the form, fill in the fields.

   For a description of the field values on the Create New Feedback form, see Create New Feedback form.

6. Select **Save**.
   The feedback is moved to the Draft state.
7. To add feedback items, select the **Items** related list.
8. Select **New**.
9. On the form, fill in the fields.

#### Create New Feedback Item form

| Field | Description |
|---|---|
| State | State of the feedback item. This field is automatically set to **Open**. |
| Context | Fields on the record on which you want to provide feedback. |
| Reviewer comments | Observations or feedback on the selected context. |
| Respondent comments | Comments or explanations provided by the respondent for the feedback. This is a read-only field for a reviewer. |

10. Select **Save**.
11. Select **Send feedback**.
    The feedback is raised and assigned to the respondent. The feedback was moved to the Assigned state.

#### Create New Feedback form

Use the Create new feedback form to provide feedback on a record or fields in a record.

See the following table for a description of the field values.

#### Create new feedback form

| Field | Description |
|---|---|
| Name | Name of the feedback. |
| Description | A brief description of the feedback. |
| Refers to ServiceNow record | Option to select a ServiceNow table record on which you want to provide feedback. Clear this option to select an external record. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Create new feedback form (continued)**

| Field | Description |
|---|---|
| Record type | Feedback integration configuration on which you want to provide feedback. This enables you to select the table defined in the configuration.<br><br>**Note:** This field appears only when the **Refers to ServiceNow record** option is selected. |
| Priority | Priority of the feedback. |
| Record | Record on which you want to provide feedback. This enables you to select the records associated in the table defined in the configuration. |
| Watch list | Individuals to be notified regarding the feedback. |
| Reviewers | |
| Reviewer group | Group that is providing the feedback. |
| Reviewer | Individual providing the feedback. This field is automatically set to your name. You can also provide feedback on behalf of someone. |
| Respondents | |
| Respondent group | Group that is responding to the feedback. |
| Respondent | Individual responding to the feedback. |
| Response | |
| Response | State of the response. This is a read-only field for a reviewer. |
| Respondent comments | Comments or explanations provided by the respondent for the feedback. This is a read-only field for a reviewer. |
| Activity | |
| Work notes | Notes or information about the feedback. For example, problems associated with the record and its possible solution. |
| Additional comments (Customer visible) | Additional information about the feedback that you want to share with the customers. |

### Create Feedback from the record side panel

Create feedback on a record or fields in a record from the record side panel using the Advanced Risk application. The feedback enables you to recommend improvements related to data integrity, compliance, operational procedures, and other pertinent areas.

**Before you begin**

Role required: sn_rvw_feedback.reviewer

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace**.
2. Select the list icon.
3. Open the record on which you want to create a Feedback.
4. In the side-panel, select the list icon.
5. Select **New**.
6. On the form, fill in the fields.

   For a description of the field values on the Create New Feedback form, see Feedback Details form.
7. Select **Save**.
   The feedback is moved to the Draft state.
8. Optional: To initiate a Sidebar discussion, select the More actions icon on the feedback, and select **Discuss**.
9. To add feedback items, select the **Add Item**.
10. On the form, fill in the fields.

#### Feedback item form

| Field | Description |
|---|---|
| Record context | Fields on the record on which you want to provide feedback. |
| Comments | Observations or feedback on the selected context. |

11. Select **Save**.
12. Select **Send feedback**.
    The feedback is raised and assigned to the respondent. The feedback is moved to the Assigned state.

#### Feedback Details form

Use the Feedback Details form to provide feedback on a record or fields in a record from the record side panel.

See the following table for a description of the field values.

#### Feedback Details form

| Field | Description |
|---|---|
| Name | Name of the feedback. |
| Description | A brief description of the feedback. |
| Reviewer group | Group that is providing the feedback. |
| Reviewer | Individual providing the feedback. This field is automatically set to your name. You can also provide feedback on behalf of someone. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Feedback Details form (continued)**

| Field | Description |
|---|---|
| Respondent group | Group that is responding to the feedback. |
| Respondent | Individual responding to the feedback. |
| Priority | Priority of the feedback. |

### Initiate a chat from Sidebar in Parallel Review and Feedback

Initiate a Sidebar chat to collaborate among different stakeholders to brainstorm solutions, clarify details, or coordinate actions regarding the feedback received.

## Before you begin

Role required: sn_rvw_feedback.reader

## Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace**.
2. Select the list  icon.
3. From the list, navigate to **Parallel Review and Feedback** and select **Feedback**.
4. Open the Feedback that you want to discuss.
5. Select **Discuss**.
   The Start a Sidebar discussion dialog box appears.
6. To initiate Sidebar discussion from the record side-panel, open the record that you want to discuss and do the following:
   a. In the side-panel, select the list  icon.
   b. Select the feedback.
   c. Select the More actions  icon on the feedback, and select **Discuss**.
7. In the Start a Sidebar discussion dialog box, fill in the fields as appropriate.

**Start a Sidebar discussion**

| Field | Description |
|---|---|
| Subject | Option to provide a title for the sidebar discussion. |
| Add participants | Options to add participants for the sidebar discussion.<br>**Note:** You can include any users with access to this record in this discussion. |
| Include a brief message for participants | Brief summary about the feedback to be discussed in the sidebar discussion. |

8. Select **Start discussion**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Respond to the feedback

Provide comments or explanations regarding the submitted feedback using the Advanced Risk application. You can either remediate or reject the feedback, provided that there's proper justification.

## Before you begin

Role required: sn_rvw_feedback.respondent

## Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **My tasks**.
2. Open the Feedback that you want to respond.
3. To respond to the feedback from the record side panel, select the list  icon on the record and do the following:
   a. Provide comments or explanations regarding the feedback submitted in the **Response** field.
   **Response** field is required to reject a feedback item.
   b. Select **Remediate** or **Reject**.
4. To respond to the feedback on the record, navigate to the **Response** section and do the following:
   a. Select the response in the **Response** field.
   b. Provide comments or explanations regarding the feedback submitted in the **Respondent comments**.
   The **Respondent comments** field becomes required when you select the response as **Rejected**.
   c. Select **Save**.
5. To respond to the feedback items, select the **Items** related list and do the following:
   The **Items** related list appears only when the reviewer adds feedback items while providing the feedback.
   a. Select the feedback items.
   b. Select the response in the **State** field.
   c. Provide comments or explanations regarding the feedback submitted in the **Respondent comments**.
   The **Respondent comments** field becomes required when you select the response as **Rejected**.
   d. Select **Save**.
6. Select **Send for review**.
   You must close all the open items to send the feedback to the reviewer.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Review and close the feedback

Review the feedback response and take further actions using the Advanced Risk application.

#### Before you begin

Role required: sn_rvw_feedback.reviewer

#### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **My tasks**.
2. Open the Feedback that you want to review and assess the respondent's comments and response.
3. If you are satisfied with the response, you have the following choices:
   - To close the feedback, select **Close**.
   - To close the feedback with an action, select **Close and initiate an action**.

   **Note:** You can create an issue or link the feedback to an existing record to facilitate follow-up and resolution.

4. Optional: If you're unsatisfied with the response, select the more actions icon and do the following:

   a. Select **Move to draft**.
   This action clears previous responses from the respondent.

   b. Select **Ok**.

### Roles for Parallel Review and Feedback

When you integrate Parallel Review and Feedback with other applications, users must have the necessary roles to review records, capture feedback, and track the closure of feedback.

The following roles have been introduced to enable users of other applications to use the Parallel Review and Feedback:

#### Roles installed

| Role title [name] | Contained under | Description |
|---|---|---|
| sn_rvw_feedback.admin | sn_risk.admin | Users with this role can configure a feedback integration setup to define the table on which you want to use parallel review and feedback. |
| sn_rvw_feedback.reviewer | sn_risk_workspace.IT_risk_manager<br>sn_risk_workspace.operational_risk_manager | Users with this role can create feedback on a record they're reviewing, suggesting overall improvements, or changes to specific fields in the record. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed (continued)**

| Role title [name] | Contained under | Description |
|---|---|---|
| sn_rvw_feedback.respondent | sn_risk_workspace.business_user_risk_manager | Users with this role can take necessary actions and provide comments or explanations regarding the submitted feedback. |
| sn_rvw_feedback.reader | sn_risk.reader | Users with this role have read-access to feedback. |

## GRC: Metrics in Integrated Risk Management

Risk metrics are defined as a quantifiable measure that is used to track and assess the status of a specific risk. Metrics help in tracking the exposure of a risk over time.

Risk indicators are an important tool within operational risk management. Indicators facilitate the monitoring and control of risk. Therefore, they may be used to support a range of operational risk management activities and processes, such as risk identification, risk and control assessments, the implementation of effective risk appetite, and the risk management and governance frameworks. Indicators only support one type of results called Pass or Fail and do not support data types such as number, percentage, or monetary amount. Metrics provide better escalation and notification mechanism for indicators, allow specific definition of data owners, and the classification of the indicators.

The key benefits of metrics are as follows.

- Provides continuous visibility into risk and control performance.
- Alerts respective owners about change of risk and control performance.
- Automates metric data collection tasks saving time for organization.
- Efficiently monitors and sharing of risk information across the organization.

### Uses of the GRC: Metrics in ESG Management and IRM

The GRC: Metrics application is used by various applications such as Integrated Risk Management and ESG Management.

Risk management and ESG (Environmental, Social, and Governance) are concepts that intersect in several ways, with ESG referring to the criteria used by investors to evaluate a company's sustainability. ESG factors consider issues such as climate change, human rights, diversity and inclusion, corporate governance, and supply chain management, among others. Risk management involves identifying, assessing, and mitigating risks that may affect an organization's ability to achieve its objectives, including financial, operational, and reputational risks, among others. The relationship between risk management and ESG is strong since poorly managed ESG factors can create significant risks for companies. For example, a company with poor environmental practices may face legal and regulatory, reputational, and operational risks. Similarly, a company with weak governance practices may face legal and reputational risks, as well as risks related to conflicts of interest and poor decision-making. By integrating ESG factors into their risk management processes, companies can identify and mitigate these risks, leading to more sustainable and resilient business models. For example, a company that identifies and mitigates its environmental risks may reduce its exposure to future environmental regulations, while a company that improves its governance practices may reduce its exposure to reputational and legal risks. Therefore, companies that effectively manage their ESG risks can improve their overall risk

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

management capabilities, create long-term value, and ensure the sustainability of their business models.

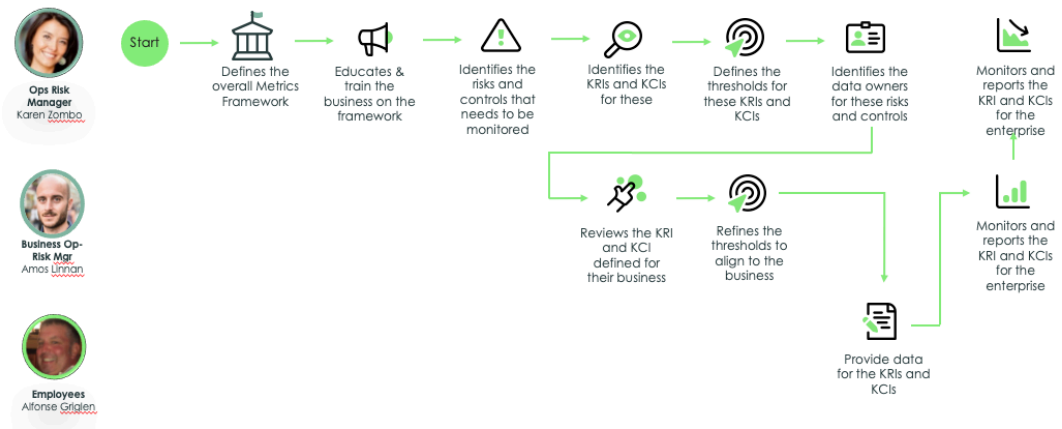
## Types of metrics

The following are the types of metrics.

- Key risk indicators (KRIs): These indicators identify the amount of exposure to a given risk or set of risks. Examples of KRIs are: Staff morale determined through employee surveys, number of hacks attempted on IT, number of negative social media posts following a loss event and so on.
- Key control indicators (KCIs): These indicators identify the effectiveness of the controls that have been implemented to reduce or mitigate a given risk exposure.
- Key performance indicators (KPIs): These indicators show how effectively the risk exposure is managed. These indicators show the achievement against objectives.

The following image shows the metrics workflow.

**Workflow of metrics**




## Difference between indicators and metrics

Indicators are used as automated control tests or assessments while metrics are used as KRIs and KCIs monitoring tool. The following table lists the differences between an indicator and a metric.

**Indicators versus metrics**

| GRC Indicators | Metrics |
|---|---|
| Used for continuous monitoring of risks and controls and for collecting supporting data. | Used to measure the degree to which a system, component, or process, possesses a given attribute. |
| Can be used to monitor a risk or control. | Can be used to measure any GRC object. |
| Can have only binary values such as pass or fail. | Can have any value: Quantitative (numbers) or Qualitative (text). |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Exploring GRC: Metrics

A metric is used to measure and evaluate the effectiveness of your organizational processes. A metric or a combination of metrics can provide an insight into a system, component, or process. The GRC: Metrics application enables other applications to assess, compare, and track the performance of the processes.

## Metrics

The GRC: Metrics application is installed automatically with the ESG Management application from the ServiceNow® Store. The user role that is responsible to read, create, and update the metric definitions and metrics is the ESG Management metrics manager (sn_esg.metrics_manager).

With the GRC: Metrics application, you can define metrics by using the metrics form. Metrics are a combination of a metric definition and an entity. Applying the metric definition to an entity creates a metric. Once the metrics are defined, data is gathered to track the effectiveness and performance of your processes. For example, consider a metric that measures the effectiveness of an incident resolution process by calculating the time it takes to resolve an incident.

Every organization has a range of data sources for building and structuring their own metric analysis. To establish a useful metric, the metrics manager must first assess and set the goals. Next, the manager sets the targets for the metrics that are integrated with their business decisions.

## Qualitative and quantitative metrics

You can classify your metrics into qualitative and quantitative measurements.

Qualitative metrics in ESG Management are derived from the subjective opinion that you form based on other information. Some examples of qualitative metrics in the ESG Management sectors are brand credibility, corporate value, and so on.

Quantitative metrics in ESG Management are the metrics that you can measure in a specific number through certain formulas. Some examples of quantitative metrics for an organization include reporting total energy use, energy use by region, and so on.

## Examples of metrics

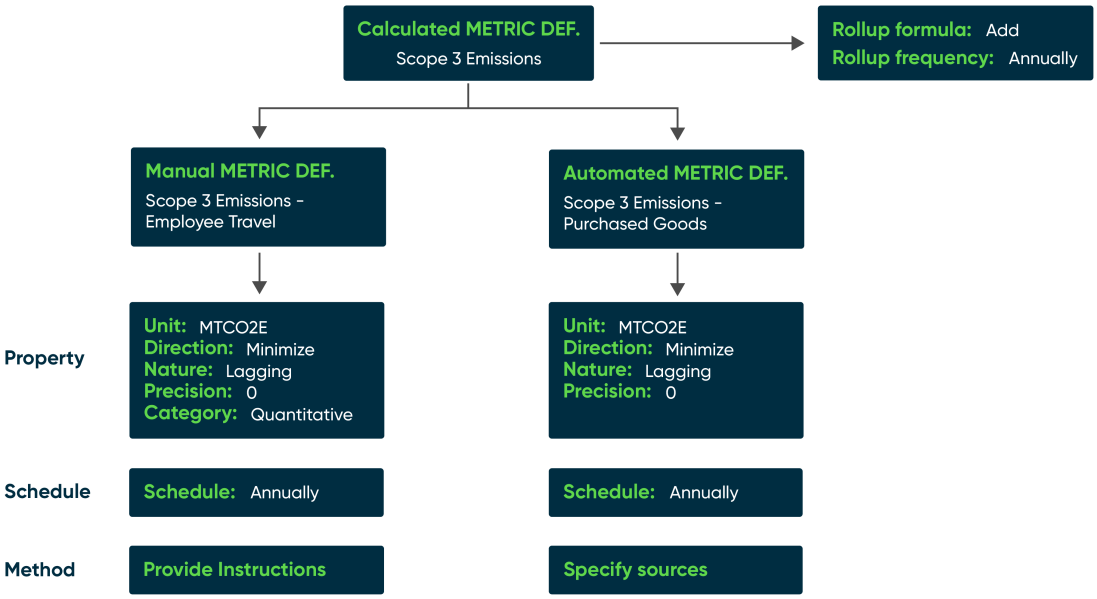
Consider the example of measuring greenhouse gas emissions for business entities in your organization. Greenhouse gas emissions are categorized into three groups called Scopes by the international Greenhouse Gas (GHG) Protocol.

You want to measure the metrics for Scope 3 Emissions for the following categories: employee travel and purchased goods. The employee travel policy applies to all the employees in the organization. You can collect the metrics for the employee travel policy manually by providing instructions in the metric definition.

On the other hand, the metrics for the purchased goods are collected automatically based on the specified conditions method, schedule, and core property in the metric definition. The metric collection process is illustrated in the following image.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Define a metric




## Metric data by entity

The metric data by entity table (sn_grc_metric_data_by_entity) includes metric definition data and metric data for entities and the aggregated data for parent entities defined in the entity hierarchy. For example, if an ESG reporting disclosure manager wants to understand the total emissions for an entire year for a particular location and if the location has sub-locations, you can also aggregate the data and use it for reporting purposes. For example, consider that your organization has a location Japan. Japan, in turn, has two sub locations, Tokyo and Kyoto. Assume that you want to find your total yearly Scope 1 emissions for the year 2022 for Japan. Using the time dimensions feature, you can aggregate your data and get a view of your total emissions for a year. You can also aggregate the data for a quarter, week, or a month depending on your reporting requirements.

### Components of GRC: Metrics

A metric consists of several components such metric definition, metric data, metric definition data, metric data tasks. All of these elements or parts contribute to the metric collection process in various ways.

## Metric definitions

A metric definition is a template-level record that helps set the core properties of a metric. These properties include the unit, direction, nature, precision, frequency of data collection, and category of the metric. The metric itself collects scores, which are then aggregated into the defined metric template. The advantage of creating and using a metric definition lies in its ability to streamline the process of creating metrics using these metric definition templates. For instance, imagine you have several business units, and you need to collect revenue data for each of them. Without a metric definition, you would have to create separate templates for every business unit and repeatedly specify the metric properties. However, by using a metric definition, you simplify this task. Once you've created the metric definition, you can easily attach your entities (business units in this case) and collect the metrics without duplicating efforts.

The GRC: Metrics application provides the following types of metric definitions:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Automated metric definition: Data is collected automatically.
- Manual metric definition: Data is collected manually.
- Calculated metric definition: Data is collected by aggregating data from other child metrics.

## Metric data

When you execute a metric, the metric data gets created. The values of metric data are copied from the metric data tasks when the metric data tasks are closed in the case of manual metric definition. For a scripted automated metric definition, the values are updated when you execute the script. For a basic automated metric definition, the values are updated from the selected table. The field **Variance (%)** shows the variation in between current period and the previous period metric data. This difference is displayed in percentage. The field **Last period data** refers to the previous period's metric data.

## Metric definition data

Metric definition data gets automatically created when the metric definition gets executed and aggregated. On the metric definition data page, the field **Variance (%)** shows the variation in between the current period and the previous period's metric definition data. This difference is displayed in percentage. The field **Last period data** refers to the previous period's metric definition data.

## Metric data tasks

Metric data tasks only apply to manual metric definitions. These tasks are generated whenever manual metric definitions are executed and the data owners provide responses for these tasks manually. You can provide responses to multiple metric data tasks using the metric data table. For more information, see Metric data table.

### Metric definition types

A metrics manager defines the metrics by creating a metric definition. A metric definition is a template-level record. In the metric definition, you set the core properties of the metric, such as unit, direction, nature, precision, and category. The metrics collect the scores, and these scores get rolled up into the metric definition.

The GRC: Metrics application provides the following types of metric definitions:

- Automated metric definition: Data is collected automatically.
- Manual metric definition: Data is collected manually.
- Calculated metric definition: Data is collected by aggregating scores from other child metrics.

These types of metric definitions are further explained in the following sections.

## Automated metric definition

In automated metric definitions, the data is collected automatically based on the conditions defined in the metric definition, such as metric properties, method, and schedule. For the method, the metrics manager specifies the source table or the script that is used for collecting the metric data and the filtering criteria to filter the metric data. See Create an automated metric definition for more information.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Manual metric definition

In manual metric definitions, the mode of data collection is manual. The data owner for a particular metric provides the metric data by going through the instructions. As the metrics manager, you have to define the metric properties, method, and schedule for the metric definition. In the method, specify the instructions for the metric definition as the metrics manager. Also, specify the data collection details such as data owner type, data owner, and approval details.

In a manual metric definition, a metric data task is generated depending upon the frequency defined in the metric definition. As a metrics manager, you can assign the task to a data owner who provides the data for the task. See Create a manual metric definition for more information. When a metric data task is created, a system generated email notification is sent to the task owner. As a metric data owner, you can provide the data for multiple metrics using the Metrics tasks module (  ). For more information, refer to Provide data for multiple metrics.

Each metric data task has a due date defined in the manual metric definition form. By default, the due date follows the schedule of 8-5. However, a risk administrator can also modify the schedule. For more information, refer to Create a new schedule. If the risk administrator wants to overwrite the schedule, then the risk administrator can modify the *sn_grc_metric.metric_data_task_schedule* property.

Both quantitative and qualitative category of metrics can be created using the manual metric definition.

It is possible to convert a manual metric definition to an automated metric definition and an automated metric definition to a manual metric definition. In the event that a manual metric definition has open tasks, it is necessary to first close them prior to converting the manual metric definition.

## Calculated metric definition

A calculated metric definition calculates the scores from its children. It can include the automated and manual metric definitions, metrics (quantitative), and other calculated metric definitions of identical frequency. As the metrics manager, you have to specify how you want to calculate the metric definitions score and how frequently you want to calculate them.

The calculated metric definition rolls up the scores from its children. The rollup property defined in the calculated metric definition consists of a rollup formula and schedule for the rollup frequency. A calculated metric definition can include those automated and manual metric definitions, and metrics as its children which are of the same frequency as that of the parent calculated metric definition. See Create a calculated metric definition for more information.

## Applying the metric definition to the entities

You can apply the metric definitions to the entities in your organization. Instead of defining the metric for each entity, you can define the metric definition once and then apply that metric definition to your entities.

For example, assume you want to measure the greenhouse gas emissions for the entities in your organization. Defining the metric for each entity is a time-consuming process. By creating a metric definition, you can define the metric once and then apply that metric definition to your entities.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following illustration shows how you can apply the metric data definition to an entity. If you have an automated metric definition for the purchased goods metric category, the metric can be applied to the Products entity and IT entity in your organization. If you have a manual metric definition such as Employee Travel, the metric can be applied to the Enterprise entity in your organization as the travel policy applies to everyone across the enterprise.

**Apply the metric data definition to an entity**




### Thresholds in Integrated Risk Management

In the context of metrics, thresholds refer to predetermined values or limits used to assess the performance of a metric. These thresholds are typically defined based on specific criteria or objectives and serve as reference points to determine whether the measured value or performance meets, exceeds, or falls below the desired level.

The three colors of thresholds—red, amber, and green—are commonly used to indicate different levels of performance or status. These colors indicate the status where green signifies the metric is performing well according to expectation, amber signals caution or warning, and red signifies a critical situation. For instance, consider a scenario where you have established a metric definition aimed at reducing credit risk, with the metric direction set to Minimize. In this case, the metric values should be lower than the specified threshold value. This requirement arises from the intention to prevent pollution from increasing and instead promote its reduction. If the metric value is higher than the defined limit, the value would appear in red or amber. Thresholds only apply to quantitative metric definitions.

## Types of threshold

There are two types of threshold for a metric.

- Static: A static threshold for a metric or a metric definition refers to a fixed value used as a limit for tracking a metric.
- Dynamic: Dynamic thresholds are specified in percentages. This means that the percentage variance is calculated based on two factors: direction and the previous data.

  For example, in June 2023, the attrition rate is 12% based on the industry average, indicating a relatively low level of risk. The objective is to minimize attrition risk, so any increase in the metric value is considered undesirable. In July 2023, new metric data is collected, and it shows that the attrition risk metric has deviated by 5%. To evaluate the significance of this increase, you can define different thresholds representing various levels of change. These thresholds are expressed as percentage differences from the previous period's data, in this case, from June 2023. For example, the organization sets a threshold range of 5% to 10%. If the percentage change in the attrition risk metric between June and July falls within this range, the threshold status is classified as "amber." This indicates a moderate level of change, signaling that the metric has deviated from the desired target value but is not yet critical. However, if the percentage change in the attrition risk metric exceeds or reaches 15%, the threshold status is classified as "red." This signifies a significant

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

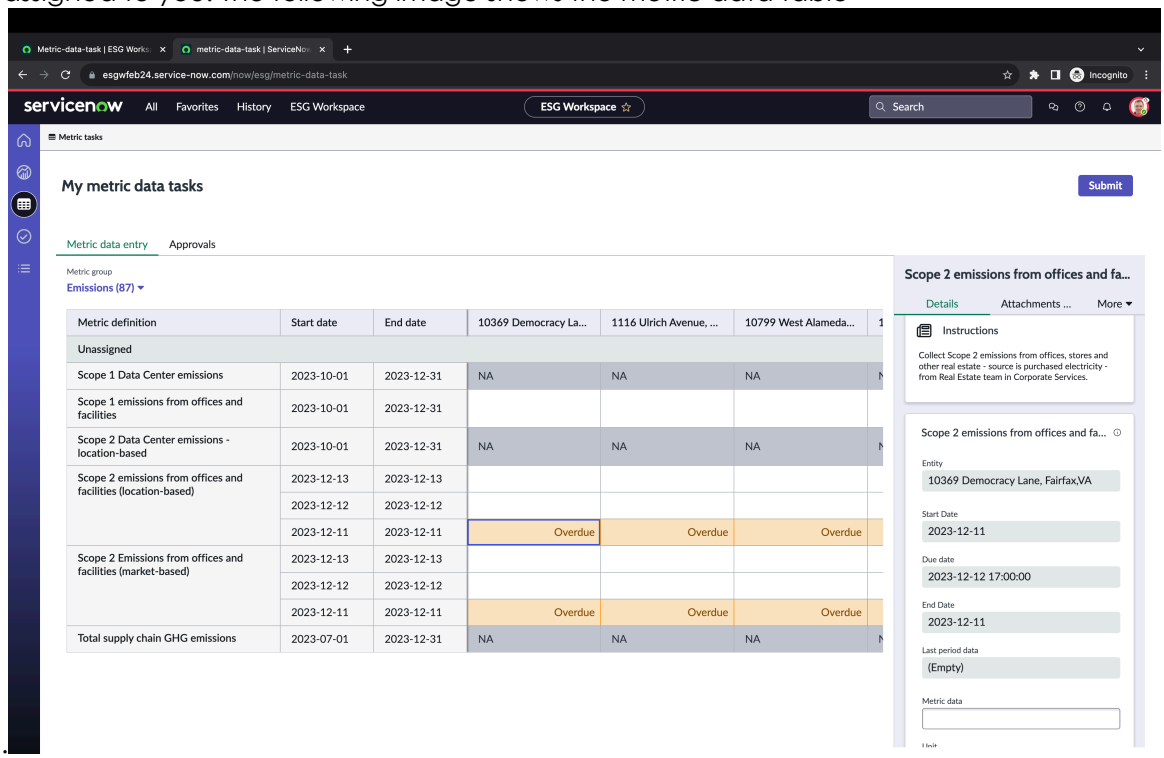
change that demands immediate attention or corrective action since it deviates greatly from the desired target value. By monitoring these threshold levels, the organization can identify and address the increasing attrition risks promptly, enabling effective risk management.

For more information, refer to Create a threshold for a metric definition.

### Metric data table

The metric data table enables data collection for metrics across the organization using an easy to use interface like a spreadsheet with a task management workflow.

As a data owner, you can access the metric data table ( ) and complete the tasks assigned to you. The following image shows the metric data table interface.




The metric data table offers the following benefits:

- Simplifies data collection across the entire organization.
- Enables you to view all the metrics that the data owner must respond to in a single place instead of navigating across multiple tasks.
- Maintains an audit trail of all changes to the data and the users who made the changes.
- Enables you to view the metrics segregated by entities.
- Gives additional information to the data owner for reference such as instructions to follow while providing the data.
- Provides the ability for the users to attach files in the Contextual side panel and attach the relevant documents and links.
- Enables ESG program managers and metrics managers to view the data submitted by the data owners and approve or reject the data with comments.
- Allows data owners to view the rejection comments in the Activity tab.
- Helps you to view how the past three data for quantitative metrics is trending.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Provides a filter to see metric groups that have open tasks and displays the number of open tasks in parentheses.
- Allows you to see the approvers of your task and the approval status.
- Displays the percentage variance of data when compared to the data of the previous period.
- Displays the threshold status if the metric exceeds the threshold.
- Enables you to view the last period's data.

## Configuring metrics

You can configure GRC: Metrics to meet the needs of your organization.

As a metrics administrator, you can do the following:

- Create a manual metric definition
- Create a calculated metric definition
- Create an automated metric definition
- Update a metric
- Create a metric unit
- Create a metric
- Create a threshold for a metric definition

### Create a manual metric definition

Create a manual metric definition to collect the data for a metric.

#### Before you begin

Role required: sn_grc_metric.manager, sn_risk.user, and sn_compliance.user

#### About this task

In the manual metric definition, the mode of data collection is manual. An option is available to set up the qualitative and quantitative metrics.

**Note:** The forms for creating an automated metric definition or a manual metric definition point to the same sn_grc_metric_definition table. The difference between the two forms is the method of the collection.

#### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Lists** > **Metrics** > **Manual metric definitions**.
2. Click **New**.
3. On the form, fill in the fields.
   For information about the fields, refer to Manual metric definition fields.
4. Click **Save**.

#### Result

The metric definition is saved in the Metric definitions list.

#### What to do next

You can associate an entity type, create metrics, and add citations to the metric definition. See Update a metric definition for more information.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Manual metric definition fields

Detailed explanation of the fields on the manual metric definition form.

#### New manual metric definition form

| Field | Description |
|---|---|
| Basic details | |
| Name | Name of the manual metric definition. For example, `Number of incidents`. |
| Active | Option to mark the manual metric definition as active. |
| Description | Brief description of the manual metric definition. |
| Category | Category of the metrics data. The choices are as follows:<br>• **Qualitative**: Qualitative data is intangible and non-numerical in nature. It's defined by the characteristics of a process or business activity.<br>• **Quantitative**: Quantitative data is tangible and numerical in nature. It's defined by the numbers or key performance indicators.<br>**Note:** This fields **Nature**, **Direction**, **Precision**, and **Unit** are only displayed only when the category of the manual metric definition is **Quantitative**. |
| Aggregation method | Method used to calculate the metric data for all the entities. For example, if you have a metric that you want to measure for multiple entities such as people, departments, or regions, you might want to know how to calculate the scores for each entity into a single score that represents the overall performance. Your choice of aggregation method depends on your goal of metric collection. For example, if you are interested in overall performance and want to account for differences in scale or size between entities, the sum or average may be more appropriate. If you are interested in identifying the best-performing entity, the maximum may be more appropriate, while if you are interested in identifying the worst-performing entity, the minimum may be more appropriate. The aggregation happens across time periods based on the frequency defined in the metric definition. If the frequency is monthly, the calculation will |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New manual metric definition form (continued)**

| Field | Description |
|---|---|
| | take place every month. The four choices for aggregation methods are as follows:<br>• **Sum**: The metric data for all entities are added together to create a single score.<br>• **Average**: The metric data for all entities are averaged to create a single score.<br>• **Maximum**: The highest metric data among all entities is used as the single score.<br>• **Minimum**: The lowest metric data among all entities is used as the single score. |
| Unit | Unit for the manual metric definition. |
| Precision | Number of decimal places after the decimal point on a score. This field is automatically set to **0**.<br>When the Precision is set to 0, the result is rounded to the nearest whole number. For example, if a metric definition with Precision 0 calculates the values 7 + (5 / 2), the result rounds up to 10.<br>When the Precision is set to greater than 0, the result is rounded to the nearest decimal point for the given precision. For example, Precision 1 rounds a result of 4.45 as 4.5. |
| Frequency | Frequency at which the metric definition should collect the scores. The choices are as follows:<br>• **Daily**<br>• **Weekly**<br>• **Monthly**<br>• **Quarterly**<br>• **Semi-annually**<br>• **Annually** |
| First run date | Start date of the metric definition execution for the collection of data according to the frequency. This field appears on when the **Category** field is set to **Quantitative**. |
| Data collection | |
| Data owner type | Type of the data owner responsible for the manual metric definition. The choices are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New manual metric definition form (continued)**

| Field | Description |
|---|---|
| | • **User**<br>• **User group** |
| Data owner | Data owner responsible for the manual metric definition. Select a data owner from the list. |
| Instructions | Instructions for the data owner. Method of collection for the manual metric definition. |
| Approval required | Option to indicate if an approval is required for the manual metric definition.<br>**Note:** When the **Approval required** option is enabled, the **Approver type** and **Approver** fields are displayed. |
| Approver type | Type of the approver of the metric definition. The choices are as follows:<br>• **User**<br>• **User group** |
| Approver | Approver user or approver group that is responsible to approve the metric definition. The choices are as follows:<br>• **Approver**: Displayed when the User option is selected.<br>• **Approver group**: Displayed when the User option is selected. |
| Metric Properties | |
| Type | Method used to determine if the score is collected manually or in an automated manner. The choices are as follows:<br>• **Automated**<br>• **Manual**<br>Select **Manual**. |
| Enterprise Owner Type | Type of enterprise owner responsible for the manual metric definition. The choices are as follows:<br>• **User**<br>• **User group** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New manual metric definition form (continued)**

| Field | Description |
|---|---|
| Direction | Direction that you want to see the metric in. The choices are as follows:<br>• **None**: If you don't want any change in the metric direction, select this option.<br>• **Minimize**: If the desired metric direction is downward, select this option.<br>• **Maximize**: If the desired metric direction is upward, select this option.<br>• **Milestone**: When the metric direction isn't applicable, but the metric is tracked against a milestone, select this option. |
| Group | Area that the metric relates to. |
| Reporting classification | Tag used to categorise the metric. |
| Due date offset | Number of days after the schedule end date when the metric data task becomes overdue. For example, if the frequency of a metric definition is monthly and if the you enter `15` in this field, then the due date for metric data task will be overdue 15 days after the month ends. |
| Enterprise owner | Enterprise owner of the manual metric definition. |
| Nature | Nature of the manual metric definition. The choices are as follows:<br>• **None**: If you don't want any change in the metric direction, select this option.<br>• **Leading** (Predictive) Metric: Is predictive and helps anticipate future outcomes. In this case, the company may use a leading metric related to GHG emissions, such as the amount of energy consumed per production unit. By tracking energy consumption, the company can predict its future GHG emissions based on the energy sources used and the efficiency of its production processes. This leading metric enables the company to proactively identify areas for improvement and make informed decisions to reduce emissions.<br>• **Lagging** (Measures Impact) Metric: Measures the impact of past actions or events. In our example, a lagging metric related to GHG emissions could be the total emissions produced by the company in a given year. This metric provides an |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New manual metric definition form (continued)**

| Field | Description |
|---|---|
| | assessment of the company's historical environmental impact. By monitoring this metric over time, the company can evaluate the effectiveness of its emission reduction efforts and identify areas where further improvements are needed. Lagging metrics help measure the outcomes of past actions and inform future strategies.<br>• **Current** metric: Monitors ongoing processes and identifies real-time improvement areas. For GHG emissions, a current metric could be the emissions intensity, which measures the emissions generated per unit of production. By tracking emissions intensity, the company can identify specific areas within its operations that contribute to higher emissions. This metric helps the company identify real-time improvement opportunities, such as optimizing energy usage, implementing energy-efficient technologies, or adopting renewable energy sources. |
| Subgroup | Subgroup that the metric relates to |
| Key metric | Option to indicate if it's a key metric for your business. |
| Confidentiality | |
| **Note:** This section only appears when:<br>• The *sn_grc.enable_record_confidentiality* property is enabled under GRC properties.<br>• The record is in **Draft** state. | |
| Confidential | Option to mark the record as confidential. |
| Allowed users | Users who can view the record.<br>**Note:** By default, the logged in user is added to the list of confidential users. |
| Allowed groups | Groups that can view the record. |

### Create an automated metric definition

Create an automated metric definition to collect the data for a metric. A metric definition specifies the method and key properties of the metric, such as the unit, direction, or nature of the metric.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_grc_metric.manager, sn_risk.user, and sn_compliance.user

### About this task
In automated metric definitions, the data is collected automatically based on the conditions that you define in the metric definition. In the condition, specify the tables that are used for collecting the metric data.

### Procedure
1. Navigate to **All** > **Risk** > **Risk Workspace** > **Lists** > **Metrics** > **Automated metric definitions**.
2. Click **New**.
3. On the form, fill in the fields.
   For information on the fields of the form, see Automated metric definition fields.
4. Click **Save**.

> **Note:** In the new automated metric definition form, only the **Details** tab is displayed. After a new automated metric definition is created, additional related lists are displayed with the **Details** tab in the form.

### Result
The automated metric definition is saved in the Metric definitions list.

### What to do next
You can associate an entity type, create metrics, and add citations to the metric definition. See Update a metric definition for more information.

#### Automated metric definition fields

The fields of the automated metric definition form are explained in this topic.

**New automated metric definition form**

| Field | Description |
|---|---|
| Basic details | |
| Name | Name of the automated metric definition. For example, `Number of incidents`. |
| Active | Option to mark the automated metric definition as active. |
| Description | Brief description of the automated metric definition. |
| Unit | Unit for the automated metric definition. You can define the units in which the data is shown. |
| Aggregation method | The Aggregation method refers to the method used to calculate the metric data for all the entities. For example, if you have a metric that you want to measure for multiple entities such as people, departments, or regions, you might want to know how to calculate the data for each entity into a single score that represents the overall performance. Your choice of aggregation |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New automated metric definition form (continued)**

| Field | Description |
|---|---|
| | method depends on your goal of metric collection. For example, if you are interested in overall performance and want to account for differences in scale or size between entities, the sum or average may be more appropriate. If you are interested in identifying the best-performing entity, the maximum may be more appropriate, while if you are interested in identifying the worst-performing entity, the minimum may be more appropriate. The aggregation happens across time periods based on the frequency defined in the metric definition. If the frequency is monthly, the calculation will take place every month. The four choices for aggregation methods are as follows:<br>• **Sum**: The metric data for all entities are added together to create a single score.<br>• **Average**: The metric data for all entities are averaged to create a single score.<br>• **Maximum**: The highest metric data among all entities is used as the single score.<br>• **Minimum**: The lowest metric data among all entities is used as the single score. |
| Class | Class to which the metric definition belongs. The choices are as follows:<br>• **KPI**: Indicates how well the risk exposure is managed against objectives. Use this option to add entities and additional entities to the metric definition.<br>• **KRI**: Indicates the amount of exposure to a given risk or set of risks. Use this option to add risks and risk statements to the metric definition. This option is available if the Advanced Risk plugin is activated.<br>• **KCI**: Indicates the effectiveness of any controls that have been implemented to reduce or mitigate a given risk exposure. Use this option to add controls and control objectives to the metric definition. This option is available if the Policy and Compliance Management plugin is activated. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New automated metric definition form (continued)**

| Field | Description |
|---|---|
| | **Important:** This field appears only when the metric definition is created from the IRM suite of applications. It does not appear for Environmental, Social, and Governance Management. |
| Precision | Number of decimal places after the decimal point on a score.<br><br>When an indicator has a Precision of 0, the indicator rounds the result to the nearest whole number. For example, if an indicator with Precision 0 calculates the values 7 + (5 / 2), the indicator rounds the result up to 10.<br><br>When an indicator has a Precision greater than 0, the indicator rounds to the nearest decimal point for the given precision. For example, an indicator with Precision 1 rounds a result of 4.45 as 4.5. |
| Frequency | Collection frequency with which the metric is executed. Indicates how often the metric definition should collect the data. The choices are as follows:<br>• **Daily**<br>• **Weekly**<br>• **Monthly**<br>• **Quarterly**<br>• **Semi-annually**<br>• **Annually** |
| First run date | Start date for the collection frequency schedule for the automated metric definition. |
| Data collection | |
| Method Type | Type of automated metric. The choices are as follows:<br>• **Basic**: Indicates using aggregation methods such as sum, average, maximum, minimum, and count distinct.<br>• **Scripted**: Indicates using a script to collect the data. This option can be used when, for example, you want to collect data from multiple tables. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New automated metric definition form (continued)**

| Field | Description |
|---|---|
| | • **External Source**: Indicates that the data will be collected from external sources. For example, if you want to source data about the number of employees in your organization and their gender ratio, you can obtain the information from an external source such as Workday which is an application that stores human resources data.<br><br>**Note:** If you select **Scripted**, you must save the form and select **Add script** to add your script. Only users with the sn_grc_metric.developer role can add scripts. |
| Table | Table from which data is obtained for the metrics. This field only appears if the **Method Type** field is set to **Basic**. |
| Criteria | Condition for the record from which data is collected. Build a filter by adding conditions that contain a field, operator, and values and then click **Set**. For example, you can build a condition that you want to collect data for only those incidents the due date for which is in the current month.<br><br>**Note:** Select a value for the **Table** field before modifying this field. |
| Aggregate | Method or the calculation used to aggregate the data from the chosen table. When an option is selected in the **Aggregate** field, a new **Aggregation Field** is displayed next to the **Aggregate** field. The **Aggregation Field** displays the selected record. The choices for the **Aggregate** field are as follows:<br><br>• **Count**: Count of the number of records that are obtained from the chosen table. For example, if you want a count of the incidents, you can select this option.<br><br>**Note:** The **Aggregation Field** is not displayed when **Count** is selected.<br><br>• **Sum**: Sum of the column that is selected in the **Aggregation Field**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New automated metric definition form (continued)**

| Field | Description |
|---|---|
| | • **Average**: Average of the values of the column that is selected in the **Aggregation Field**.<br>• **Maximum**: Maximum of the values of column that is selected in the **Aggregation Field**.<br>• **Minimum**: Minimum of the values of the column that is selected in the **Aggregation Field**.<br>• **Count Distinct**: Number of groups in the result set that is grouped by the **Aggregation Field**. |
| Table field | Column or field of the table that is selected in the **Table** field. For example, you can select the **Caller** column in the Incident table. This selection enables you to understand that which callers are associated with the Incident table and compare them with the callers of your entities.<br>**Note:** Select a table before modifying this field. |
| Aggregation field | Column or field from the table that is selected in the **Table** field on which the aggregation must be performed.<br>**Note:** This field does not appear if **Count** is selected in the **Aggregate** field. |
| Entity field | Column or field from the entity table. The entities are matched based on the field selected in the **Table field** and the field selected in the **Entity field**. This field is automatically set to **Applies to record**. In the context of the Incident table in this procedure, this field enables you to compare, for example, which particular incident has been logged by which caller. |
| Metric Properties | |
| Type | Method used to determine if the data is collected manually or in an automated manner. The choices are as follows:<br>• **Automated**<br>• **Manual** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New automated metric definition form (continued)**

| Field | Description |
|---|---|
| | Select **Automated** because the procedure is to create an automated metric definition. |
| Enterprise Owner Type | Type of enterprise owner who is responsible for the automated metric definition. The choices are as follows:<br>• **User**<br>• **User group** |
| Direction | Direction that you want to see the metric in. The choices are as follows:<br>• **None**: If you don't want any change in the metric direction, select this option.<br>• **Minimize**: If the desired metric direction is downward or descending, select this option. For example, you want to minimize the fuel consumption.<br>• **Maximize**: If the desired metric direction is upward or ascending, select this option. For example, you want to maximize the use of natural resources in your organization.<br>• **Milestone**: When the metric direction isn't applicable, but the metric is tracked against a milestone, select this option. For example, if your organization is going to launch a new renewable energy product in the market, the upcoming launch date is considered as a milestone. |
| Group | Area that the metric relates to. For example, the,metric may be related to the area of gender diversity, energy, water consumption, and so on. |
| Reporting classification | Tag used to categorise the metric. |
| Enterprise owner | User who is the owner of the metric and is responsible for the metric. For example, for a metric such as revenue collection, the vice president or the general manager of the business unit could be the enterprise owner. |
| Nature | Nature of the automated metric definition. The choices are as follows:<br>• **None**: If you don't want any change in the metric direction, select this option.<br>• **Leading** (Predictive) Metric: Is predictive and helps anticipate future outcomes. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New automated metric definition form (continued)**

| Field | Description |
|---|---|
| | In this case, the company may use a leading metric related to GHG emissions, such as the amount of energy consumed per production unit. By tracking energy consumption, the company can predict its future GHG emissions based on the energy sources used and the efficiency of its production processes. This leading metric enables the company to proactively identify areas for improvement and make informed decisions to reduce emissions.<br>• **Lagging** (Measures Impact) Metric: Measures the impact of past actions or events. In our example, a lagging metric related to GHG emissions could be the total emissions produced by the company in a given year. This metric provides an assessment of the company's historical environmental impact. By monitoring this metric over time, the company can evaluate the effectiveness of its emission reduction efforts and identify areas where further improvements are needed. Lagging metrics help measure the outcomes of past actions and inform future strategies.<br>• **Current** metric: Monitors ongoing processes and identifies real-time improvement areas. For GHG emissions, a current metric could be the emissions intensity, which measures the emissions generated per unit of production. By tracking emissions intensity, the company can identify specific areas within its operations that contribute to higher emissions. This metric helps the company identify real-time improvement opportunities, such as optimizing energy usage, implementing energy-efficient technologies, or adopting renewable energy sources. |
| Subgroup | Subgroup that the metric relates to. |
| Key metric | Option to indicate if the metric is a key metric for your business. |
| Confidentiality | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New automated metric definition form (continued)**

| Field | Description |
|---|---|
| **Note:** This section only appears when:<br>• The *sn_grc.enable_record_confidentiality* property is enabled under GRC properties.<br>• The record is in **Draft** state. | |
| Confidential | Option to mark the record as confidential. |
| Allowed users | Users who can view the record.<br>**Note:** By default, the logged in user is added to the list of confidential users. |
| Allowed groups | Groups that can view the record. |

### Create a calculated metric definition

Create a calculated metric definition by aggregating the automatic metric definition and the manual metric definition.

#### Before you begin

Role required: sn_grc_metric.manager, sn_risk.user, and sn_compliance.user

#### About this task

Add the automatic metric definition and the manual metric definition as children to the parent calculated metric definition. Specify the frequency and the method to aggregate the two metric definitions.

#### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Lists** > **Metrics** > **Calculated metric definitions**.
2. Click **New**.
3. On the form, fill in the fields.
   For information about the fields of the form, refer to Calculated metric definition form
4. Click **Save**.

#### Result

The metric definition is saved in the Metric definitions list.

#### What to do next

You can associate an entity type, create metrics, and add citations to the metric definition. See Update a metric definition for more information.

### Calculated metric definition form

Field of the calculated metric definition form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### New calculated metric definition form

| Field | Description |
|---|---|
| Basic details | |
| Name | Name of the calculated metric definition. For example, `Number of employees`. |
| Active | Option to mark the calculated metric definition as active. |
| Description | Brief description of the calculated metric definition. |
| Unit | Unit for the metric definition. You can define the units in which the scores are shown. The most commonly used units are provided by default. |
| Precision | Number of decimal places after the decimal point on a score. This field is automatically set to **0**.<br><br>When the Precision is set to 0, the result is rounded to the nearest whole number. For example, if a metric definition with Precision 0 calculates the values 7 + (5 / 2), the result rounds up to 10.<br><br>When the Precision is set to greater than 0, the result is rounded to the nearest decimal point for the given precision. For example, Precision 1 rounds a result of 4.45 as 4.5. |
| Frequency | Frequency for the calculated metric definition. This field indicates how often the metric definition should roll up the scores. The choices are as follows:<br>• **Daily**<br>• **Weekly**<br>• **Monthly**<br>• **Quarterly**<br>• **Semi-annually**<br>• **Annually** |
| Calculation | |
| Calculation level | Level at which the calculation is performed. The choices are as follows:<br>• **Metric definition**: If you calculate the data at the metric definition level, then the data across all child metric definitions or child metrics is used for calculation. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New calculated metric definition form (continued)**

| Field | Description |
|---|---|
| | • **Entity**: If you calculate data at the entity level and specify the calculation method using the formula builder, then the common entities across all the child metric definitions are matched and the data is calculated for each entity. To aggregate the data to get an overall score at the metric definition level, select **Entity**. |
| Aggregation method | Method to aggregate the metric score at the entity level. The choices are as follows:<br>• **None**<br>• **Sum**<br>• **Average**<br>• **Maximum**<br>• **Minimum**<br><br>This field only appears when the **Calculation level** field is set to **Entity**. |
| Metric Properties | |
| Enterprise Owner Type | Enterprise owner responsible for the calculated metric definition. The choices are as follows:<br>• **User**<br>• **User group** |
| Enterprise owner | Enterprise owner of the metric definition. |
| Direction | Direction that you want to see the metric in. The choices are as follows:<br>• **None**: If you do not want any change in the metric direction, select this option.<br>• **Minimize**: If the desired metric direction is downward, select this option. For example, if you want to minimize the carbon emission from the datacenters.<br>• **Maximize**: If the desired metric direction is upward, select this option. For example, if you want to maximize the use of energy-efficient resources in your organization.<br>• **Milestone**: When the metric direction is not applicable, but the metric is tracked against a milestone, select this option. For example, if your organization has a goal |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New calculated metric definition form (continued)**

| Field | Description |
|---|---|
| | to use 100% renewable energy by the end of 2029, the upcoming date for the goal is considered as a milestone. |
| Nature | Nature of the calculated metric definition. The choices are as follows:<br>• **None**:<br>• **Leading** (Predictive) Metric: Is predictive and helps anticipate future outcomes. In this case, the company may use a leading metric related to GHG emissions, such as the amount of energy consumed per production unit. By tracking energy consumption, the company can predict its future GHG emissions based on the energy sources used and the efficiency of its production processes. This leading metric enables the company to proactively identify areas for improvement and make informed decisions to reduce emissions.<br>• **Lagging** (Measures Impact) Metric: Measures the impact of past actions or events. In our example, a lagging metric related to GHG emissions could be the total emissions produced by the company in a given year. This metric provides an assessment of the company's historical environmental impact. By monitoring this metric over time, the company can evaluate the effectiveness of its emission reduction efforts and identify areas where further improvements are needed. Lagging metrics help measure the outcomes of past actions and inform future strategies.<br>• **Current** metric: Monitors ongoing processes and identifies real-time improvement areas. For GHG emissions, a current metric could be the emissions intensity, which measures the emissions generated per unit of production. By tracking emissions intensity, the company can identify specific areas within its operations that contribute to higher emissions. This metric helps the company identify real-time improvement opportunities, such as optimizing energy |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New calculated metric definition form (continued)**

| Field | Description |
|---|---|
| | usage, implementing energy-efficient technologies, or adopting renewable energy sources. |
| Group | Area that the metric relates to. For example, the,metric may be related to the area of energy, water emissions, and so on. |
| Reporting classification | Tag used to categorise the metric. |
| Subgroup | Subgroup that the metric relates to. |
| Key metric | Option to indicate if it is a key metric for your business. |
| Confidentiality | |
| **Note:** This section only appears if the following situations are true:<br>• The *sn_grc.enable_record_confidentiality* property is enabled under GRC properties.<br>• The record is in Draft state. | |
| Confidential | Option to mark the record as confidential. |
| Allowed users | Users who can view the record.<br>**Note:** By default, the logged in user is added to the list of confidential users. |
| Allowed groups | Groups that can view the record. |

### Formula building in a calculated metric definition

In a calculated metric definition, you can create formulas to perform calculations for any data that you may require.

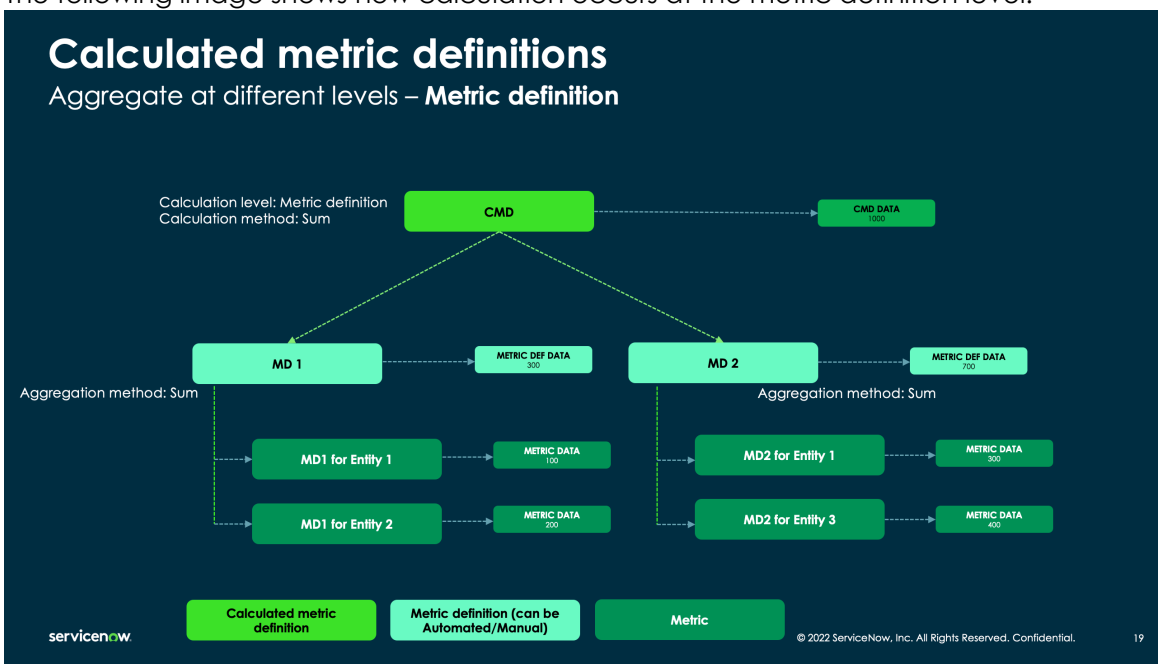
A formula consists of operands, operators, and functions. For example, if you want to calculate the total employee count from two metric definitions namely number of male employees and number of female employees, then the selected metric definitions are the operands and the operator is the symbol or function that performs a specific operation on the operands to obtain a result. Examples of operators include addition (+), subtraction (-), multiplication (*), and division (/).

When you build a formula in a calculated metric definition, you can choose to build it at either the metric definition level or at the entity level. Before you save the calculated metric definition form and build the formula for metric definition score calculation, you must specify the calculation level in the calculated metric definition form. The two levels are as follows:

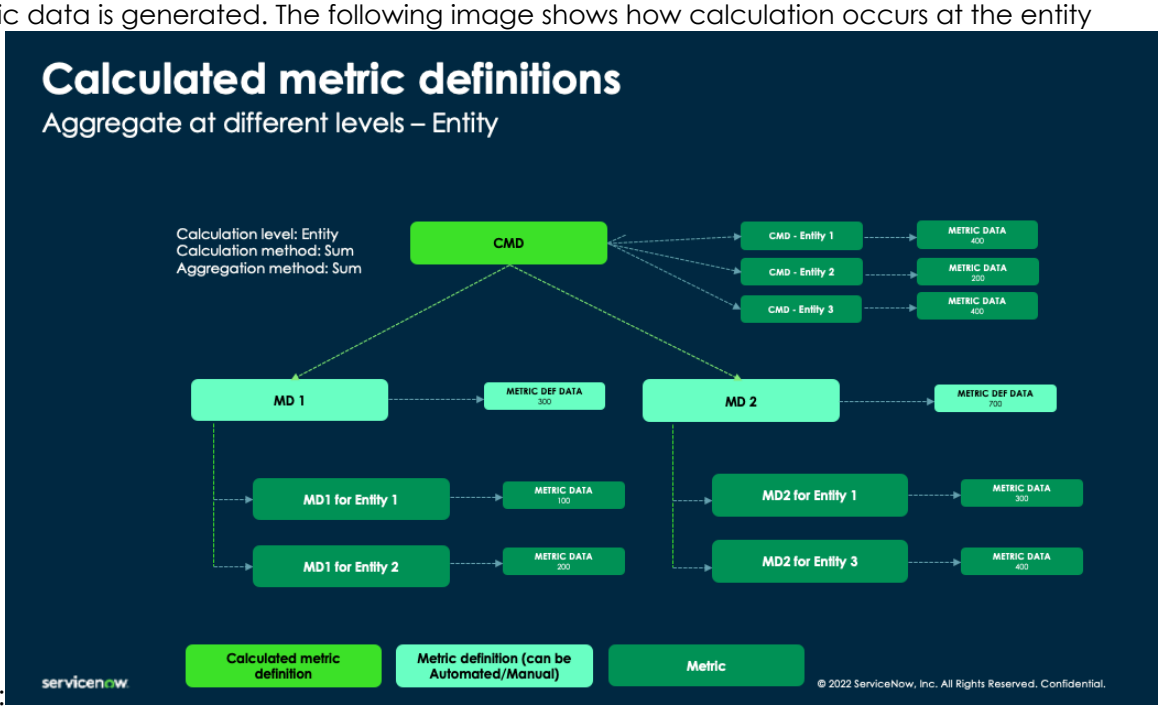
- **Metric definition**: If you select **Metric definition** in the **Calculation level** field, then the data across all child metric definitions or child metrics is used for calculation. When you select **Execute**, the formula is applied and the calculated metric definition data is generated. For more information, see Configure the formula builder.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following image shows how calculation occurs at the metric definition level:




- **Entity**: If you select **Entity** in the **Calculation level** field and specify the calculation method using the formula builder, then the child metrics are created for the calculated metric definition. These metrics are created for each distinct entity that is associated with the metric definitions that have been used as operands in the formula. When you Execute the metric definition, the formula is applied and the metric data is generated. When you Aggregate the metric definition, the metric data is aggregated and the calculated metric data is generated. The following image shows how calculation occurs at the entity level:




### Specify a formula at the metric definition level to calculate a metric definition score

Specify a formula at the metric definition level. Use the formula to calculate the metric definition score. You can either use a predefined function or you can create a custom formula.

### Before you begin

Role required: admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **Risk Workspace** > **List** > **Metrics** > **Calculated metric definitions**.
2. Select and open the metric definition for which you want to specify the formula.
3. Select **Build formula**.
4. On the Build formula pop-up window, fill in the fields.
   For the descriptions of the field values, see Fields for building formula at the metric definition level.
5. If you have selected a predefined function in the **Calculation method field**, select one of the following options.

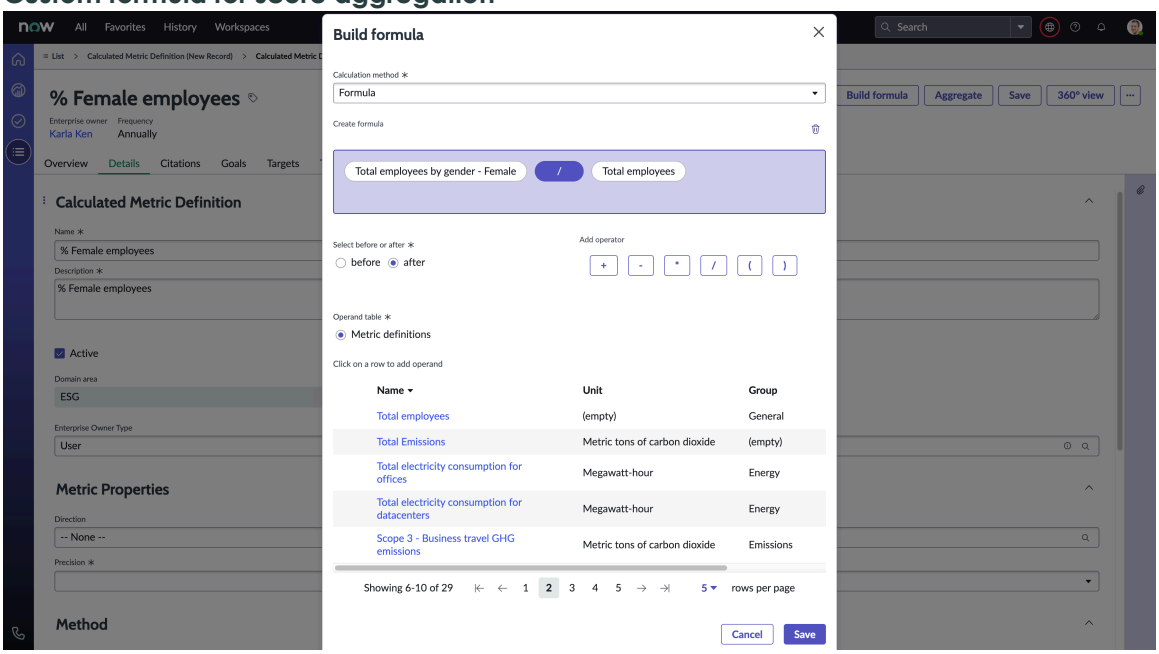
| Choice | Action |
|---|---|
| Metric definition | Select the metric definitions using which you want to calculate the metric definition score. |
| Metrics | Select the metrics using which you want to calculate the metric definition score. |

6. If you have selected **Formula** in the **Calculation method field**, select the metric definitions you want to include in the formula.
7. Select an operator and specify the operator's position using the **before** and **after** options.
8. Select **Save**.

## Example: Building a custom formula using metric definitions

Here is an example that shows a custom formula that is built using metric definitions.

### Custom formula for score aggregation




### Fields for building formula at the metric definition level

See the following table for a description of the field values.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Build formula window

| Field | Description |
|---|---|
| Calculation method | Formula to calculate the metric definition score. The choices are the following:<br>• Sum<br>• Average<br>• Maximum<br>• Minimum<br>• Formula |
| Formula text area | The metrics or the metric definitions that you include in the formula. |
| Operand table | |
| Metric definitions | Option to select the metric definitions to be included in the formula. |
| Metrics | Option to select the metrics to be included in the formula. This option is not available if the **Calculation method** field is set to **Formula.** |

### Specify formula at the entity level

Specify a formula at the entity level. Use the formula to calculate the metric definition score. You can either use a predefined function or you can create a custom formula.

## Before you begin

Ensure that in the Calculated metric definition form, the **Calculation level** field is set to **Entity**.

Role required: admin

## Procedure

1. Navigate to **All** > **Risk Workspace** > **List** > **Metrics** > **Calculated metric definitions**.
2. Select and open the metric definition for which you want to specify the formula.
3. Select **Build formula**.
4. On the Build formula pop-up window, fill in the fields.
   For the descriptions of the field values, see Fields for building a formula at the entity level.
5. If you have selected a predefined function in the **Calculation method field**, then perform the following steps:
   a. Select the **Metric definitions** option.
   b. Select the metric definitions using which you want to aggregate the metric score.
6. If you have selected **Formula** in the **Calculation method field**, select one of the following options.

| Choice | Action |
|---|---|
| Metric definitions | Select the metric definitions using which you want to aggregate the metric score. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Choice | Action |
| --- | --- |
| Emission factors | Select the emission factors using which you want to aggregate the metric score. |

7. Select an operator and specify the operators position using the **before** and **after** options.
8. Select **Save**.

### Fields for building a formula at the entity level

See the following table for a description of the field values.

**Build formula window**

| Field | Description |
| --- | --- |
| Calculation method | Formula to calculate the metric definition score. The choices are the following:<br>• Sum<br>• Average<br>• Maximum<br>• Minimum<br>• Formula |
| Formula text area | The metrics, the metric definitions, or the emission factors that you include in the formula. |
| Operand table. | |
| Metric definitions | Option to build the formula based on metric definitions. |
| Emission factors | Option to build the formula based on emission factors. This option is only available if the **Calculation method** field is set to **Formula.** |

### Update a metric definition

Update an existing metric definition to collect the new metrics. You can associate new goals, targets, and entities with the metric definition.

#### Before you begin

Role required: sn_grc.metric_manager, sn_risk.user and sn_compliance.user

#### About this task

You can use the same form for updating the automated metric definition, manual metric definition, and composite metric definition.

#### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Metrics**.
2. Select a metric definition from the list.
3. On the form, update the fields as necessary.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Update metric definitions tabs and related lists

| Field | Description |
|---|---|
| Tabs and related lists | |
| Details tab | Details of the metric, such as metric definition, metric properties, method, and schedule in the automated metric definition.<br><br>Details of the metric, such as collection method, schedule, data collection details, approval in the manual metric definition.<br><br>Details of the metric, metric properties, and roll up properties in the calculated metric definition. The fields on the Details tab are explained in the Metric definition forms. |
| Entity type | Details of the entity type to be associated with the metric. For example, provides the name, description, and conditions, such as active, need update, and processing entities. To add a new entity type, click **Add**.<br><br>**Note:** The Entity type related list is displayed only for an automated metric definition and a manual metric definition. It isn't displayed for the calculated metric definition. |
| Additional entities | Additional entities that can be associated with the metric definition. Provides details, such as name, owned by, class, and compliance score in percentage (%). To add new entities, click **Add**.<br><br>**Note:** This related list is displayed only for an automated metric definition and a manual metric definition. It isn't displayed for the calculated metric definition. |
| Child Metric Definition | Child metric definition associated with the parent metric definition. Displays the details such as name, frequency, and description of the child metric definition. To add a new child metric definition, click **Add**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** This related list is displayed only for the calculated metric definition. It isn't displayed for the automated metric definition and the manual metric definition. |
| Metrics | Details of the metrics, such as name, associated entity, and active state of the metric. To add a new metric, click **New**. |
| Citations | Details of the citations such as reference, name, authority document, description, and compliance score in percentage (%). To add a new citation, click **Add**. |
| Goals | Details of the goals, such as name, state, category, start date, end date, owner, and status. To add a new goal, click **Add**. |
| Targets | Details of the target, such as name, owner, state, status, progress, actual value, target value, and end date. To add a new target, click **Add**. |
| Metric definition data | Details of the metric definition data, such as collection frequency, collection definition, interval end date, value, and state.<br>**Note:** This related list is displayed only for an automated metric definition and a manual metric definition. It isn't displayed for the calculated metric definition. |
| Calculated metric data | Details of the calculated metric data, such as interval end date, roll up frequency, and value.<br>**Note:** This related list is displayed only for the calculated metric definition. It isn't displayed for the automated metric definition and the manual metric definition. |

4. To save the metric definition, click **Save**.
5. To calculate the composite metric data for the composite metric definition, click **Aggregate**.
   The **Aggregate** action calculates the composite metric data for the current interval end date and roll-up frequency to its parent metric definition. The composite metric data record is displayed under the Composite metric data related list. A composite metric definition score is created if it doesn't exist for the current interval.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. To delete the metric definition, click **Delete**.
7. To visually explore the 360° relationship view of the metric definition, click **360° view**.

### Create a metric

Create a metric to perform calculations on your data.

#### Before you begin

Role required: sn_grc_metric.manager, sn_risk.user, and sn_compliance.user

#### About this task

To create a metric, you need a metric definition and an entity. A metric definition defines the method for collecting the score for an entity. When a metric definition gets associated with an entity, it creates a metric.

#### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Lists** > **Metrics** > **Metrics**.
2. Click **New**.
3. On the form, fill in the fields.

**New automated metric definition form**

| Field | Description |
|---|---|
| Name | Name of the automated metric definition. For example, `Number of incidents`. |
| Description | Brief description of the automated metric definition. |
| Active | Option to mark the automated metric definition as active. |
| Class | Class to which the metric definition belongs. The choices are as follows:<br>◦ **KPI**: Indicates how well the risk exposure is managed against objectives. Use this option to add entities and additional entities to the metric definition.<br>◦ **KRI**: Indicates the amount of exposure to a given risk or set of risks. Use this option to add risks and risk statements to the metric definition. This option is available if the Advanced Risk plugin is activated.<br>◦ **KCI**: Indicates the effectiveness of any controls that have been implemented to reduce or mitigate a given risk exposure. Use this option to add controls and control objectives to the metric definition. This option is available if the Policy and Compliance Management plugin is activated. |
| Type | Method used to determine if the score is collected manually or in an automated manner. The choices are as follows: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ **Automated**<br>◦ **Manual**<br>Select **Automated**. |
| Key metric | Option to indicate if the metric is a key metric for your business. |
| Domain area | The workspace from where the metric definition is created. This field is automatically set. For example, if you create a metric definition from the Risk Workspace, then this field is set to **Risk**. |
| Enterprise Owner Type | Type of enterprise owner who is responsible for the automated metric definition. The choices are as follows:<br>◦ **User**<br>◦ **User group** |
| Metric Score Aggregation | Method used to summarize the score at the metric definition level. The choices are as follows:<br>◦ **Sum**: Sum of all active metrics.<br>◦ **Average**: Average of all active metrics.<br>◦ **Maximum**: Maximum value of all active metrics.<br>◦ **Minimum**: Minimum value of all active metrics. |
| Value | Value obtained after the metrics are executed. |
| Enterprise owner | Enterprise owner of the automated metric definition. |
| Metric Properties | |
| Direction | Direction of the automated metric definition. The choices are as follows:<br>◦ **None**: If you don't want any change in the metric direction, select this option.<br>◦ **Minimize**: If the desired metric direction is downward or descending, select this option. For example, you want to minimize the fuel consumption.<br>◦ **Maximize**: If the desired metric direction is upward or ascending, select this option. For example, you want to maximize the use of natural resources in your organization.<br>◦ **Milestone**: When the metric direction isn't applicable, but the metric is tracked |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | against a milestone, select this option. For example, if your organization is going to launch a new renewable energy product in the market, the upcoming launch date is considered as a milestone. |
| Precision | Number of decimal places after the decimal point on a score.<br><br>When an indicator has a Precision of 0, the indicator rounds the result to the nearest even, whole number. For example, if an indicator with Precision 0 calculates the values 7 + (5 / 2), the indicator rounds the result up to 10. However, if the formula calculates 2 + (5 / 2), the indicator rounds the result down to 4.<br><br>When an indicator has a Precision greater than 0, the indicator rounds to the nearest decimal point for the given precision. For example, an indicator with Precision 1 rounds a result of 4.45 as 4.5. |
| Unit | Unit for the automated metric definition. You can define the units in which the scores are shown. The most commonly used units are provided by default. |
| Nature | Nature of the automated metric definition. The choices are as follows:<br>◦ **None**<br>◦ **Leading**: If the metric is an indicator of future events, select this option. For example, consider the number of sales that a store makes on new solar batteries. This number is a leading indicator for the support requests that the store may receive in the future.<br>◦ **Lagging**: If the metric is an indicator of past events, select this option. For example, consider the number of sales that a store has made in the previous year. This number is a lagging indicator for the support requests that the store has received in the past year.<br>◦ **Current**: If the metric is an indicator of the current state of the events, select this option. For example, consider the number of sales that a store has made in the current year. This number is an indicator of the current support requests received by the store. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Method | |
| Method Type | Type of automated metric. The choices are as follows:<br>◦ **Basic**<br>◦ **Scripted**<br>**Note:** If you select **Scripted**, you must save the form and select **Add script** to add your script. Only users with the sn_grc.developer role can add scripts. |
| Table | Table that is queried for creating the automated metric definition. |
| Criteria | Condition for the record from which a score is obtained. Build a filter by adding conditions that contain a field, operator, and values and then click **Set**.<br>**Note:** Select a value for the **Table** field before modifying this field. |
| Aggregate | Method to aggregate the automated metric definition score. When an option is selected in the **Aggregate** field, a new **Aggregation Field** is displayed next to the **Aggregate** field. The **Aggregation Field** displays the selected record. The choices for the **Aggregate** field are as follows:<br>◦ **Count**: Count of the number of records that are rendered by the table query that is set in the filter criteria.<br>◦ **Sum**: Sum of the values of the parameters based on the selected value in the **Aggregation Field**.<br>◦ **Average**: Average of the values of the parameters based on the selected value in the **Aggregation Field**.<br>◦ **Maximum**: Maximum of the values of the parameters based on the selected value in the **Aggregation Field**.<br>◦ **Minimum**: Minimum of the values of the parameters based on the selected value in the **Aggregation Field**.<br>◦ **Count Distinct**: Number of groups in the result set that is grouped by the **Aggregation Field**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** The **Aggregation Field** is displayed for all the options except **Count**. |
| Reference field | Field based on which the metric data can be segregated. This field connects the entity to the selected scoring table and it calculates a score that is specific to an entity.<br>**Note:** Ensure that the table that the reference field points to matches with the table of the records that the associated entities point to, through the **Applies to** field in the entity form.<br>**Note:** It is the user's responsibility to validate the criteria mentioned in the note as the system doesn't validate it. Select a table before modifying this field. |
| Schedule | |
| Collection frequency | Collection frequency with which the metric is executed. Indicates how often the metric definition should collect the scores. The choices are as follows:<br>◦ **Daily**<br>◦ **Weekly**<br>◦ **Monthly**<br>◦ **Quarterly**<br>◦ **Semi-annually**<br>◦ **Annually** |
| Start at | Start date for the collection frequency schedule for the automated metric definition. |
| Classification | |
| Group | Area that the metric relates to. |
| Label | Tag used to categorise the metric. |
| Subgroup | Subgroup that the metric relates to. |
| Confidentiality | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| **Note:** This section only appears when:<br>◦ The *sn_grc.enable_record_confidentiality* property is enabled under GRC properties.<br>◦ The record is in **Draft** state. | |
| Confidential | Option to mark the record as confidential. |
| Allowed users | Users who can view the record.<br>**Note:** By default, the logged in user is added to the list of confidential users. |
| Allowed groups | Groups that can view the record. |

4. Click **Save**.

**Note:** After a new metric is created, the related lists along with the **Details** tab are displayed on the form. You can view the metric data overview in the **Overview** tab. The Metrics overview page displays the metrics data details when you execute a metric along with the duration for which the data is collected.

**Result**
The metric is saved in the Metrics list.

### Create a metric unit

Define the units in which the metric scores are displayed. The units can be numbers, percentages, currencies, quantities of time, or any other unit that you define. The commonly used units are provided by default.

**Before you begin**
Role required: sn_grc_metric.manager, sn_risk.user and sn_compliance.user

**Procedure**

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Metrics** > **Units**.
2. Click **New**.
3. On the form, fill in the fields.

**New metric unit form**

| Field | Description |
|---|---|
| Name | Name of the unit. For example, `$`. |
| Format | Format of the unit. For example, `{0} MWh` gives you the number of Megawatt-hours with the abbreviation MWh. |

4. To save the metric unit, click **Save**.

**Result**
The metric unit is saved in the Units list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create a unit family

Create a unit family to group similar units together. For example, the various units of distance such as miles and kilometers can be grouped. Unit families help you to organize units during unit conversion.

#### Before you begin

Role required: admin

#### About this task

Creating unit families also supports conversion of units. Sometimes, the unit in which metric data is entered may be different from the reporting unit of the metric definition. In such cases, the units must be converted. For example, the metric data may be entered in US gallons and the reporting unit in the metric definition is Liters. If US gallon and liters belong to the same unit family such as Volume, you can convert the units.

Various formulas are used to convert different units. If the reporting unit of a metric definition belongs to a unit family that has the conversion factor as **Calculated**, then the metric data tasks for that metric must be provided in the same unit as the metric definition. For example, if the reporting unit for temperature in a metric definition is Celsius, and if the conversion factor of temperature is set to **Calculated**, then all the metric data tasks for that metric definition can only be provided in Celsius. In such cases, users can specify the formula that must be used for the conversion. For more information see, Formula building in a calculated metric definition.

#### Procedure

1. Navigate to **All** > **Risk** > **Administration** > **Unit family**
2. Select **New**.
3. On the form, fill in the fields.

**Unit family form**

| Field | Description |
|---|---|
| Name | Name of the unit family. For example, `Temperature`. |
| Conversion factor | Conversion factor that must be applied when converting units from the family. The choices are as follows:<br>◦ **Direct**: Use this option if the conversion of the units in the family can be done directly. For example, you can convert kilometers to miles using direct conversion.<br>◦ **Calculated**: Use this option if the conversion formulas are complex. For example, to convert temperatures in degrees Celsius to Fahrenheit, the formula is °F = °C × (9/5) + 32. |

4. Select **Submit**.

### Convert metric data to a different unit

Convert any metric data into a preferred reporting unit.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: admin

### About this task
The preferred reporting unit for any data is specified in a metric definition. When users enter the data in a metric data task, they may do so in a unit that is different from the unit set in the metric definition. For example, a user may enter data about water usage in liters but the organization needs the report in US gallons. And therefore, the metric definition is also set to gallons. In this case, liters must be converted to US gallons.

**Note:** In the metric data task, only those units that belong to the same unit family are available for the data. Unit conversion only applies to units that have the unit family conversion factor set to **Direct**.

### Procedure
1. Navigate to **All** > **Risk** > **Administration** > **Unit Conversions**.
2. Select **New**.
3. On the form, fill in the fields.

#### Unit conversion form

| Field | Description |
|---|---|
| Name | Name of the unit conversion. For example, `Litres to gallons`. |
| From unit | Unit to convert. |
| To unit | Unit to convert to. |
| Unit family | Unit family to which the unit belongs. For example, **Volume**. |
| Value | Conversion value. For example, the conversion value from liters to gallons is `0.264172`. |

4. Select **Submit**.

#### Update a metric

Update a metric to add goals, metric data, and targets. Associate citations to the metric.

### Before you begin
Role required: sn_grc_metric.manager, sn_risk.user, and sn_compliance.user

### Procedure
1. Navigate to **All** > **Risk** > **Risk Workspace** > **Lists** > **Metrics** > **Metrics**.
2. Select a metric from the list.
3. On the form, update the fields as necessary.

#### Update metric tabs and related lists

| Field | Description |
|---|---|
| Tabs | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Name | Name for the metric. For example, `Number of incidents- ACME Asia`. |
| Description | Brief description of the metric. |
| Metric definition | Metric definition associated with the metric. |
| Entity | Entity associated with the metric. |
| Enterprise Owner Type | Enterprise owner type who is responsible for the metric. This field is automatically set to display the enterprise owner type. |
| Type | Type of the automated metric definition. This field is automatically set. |
| Active | Option to mark the metric definition as active. |
| Key metric | Option to mark the metric definition as a key metric. |
| Enterprise owner | Enterprise owner of the metric definition. This field is automatically set. |
| Metric Properties | |
| Direction | Direction of the metric definition. This field is automatically set. |
| Precision | Precision for the metric definition. This field is automatically set. |
| Unit | Unit for the metric definition. This field is automatically set. |
| Nature | Nature of the metric definition. This field is automatically set. |
| Method | |
| Table | Table that is queried for creating the metric definition. This field is automatically set. |
| Criteria | Conditions for querying the table. This field is automatically set. |
| Aggregate | Method to aggregate the metric definition. This field is automatically set. |
| Reference field | Reference field for the metric definition method. This field is automatically set. |
| Schedule | |
| Schedule | Collection frequency for the metric definition. This field is automatically set. |
| First run time | Date for the first run time. This field is automatically set. |
| Next run time | Date for the next run time. This field is automatically set. |
| Data Collection Details | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Data owner type | Data owner type such as User. |
| Data owner | Name of the user as the data owner. |
| Approval | |
| Approval required | Option to be enabled if an approval is requested for the metric. |
| Metric data tasks tab | Information about the metric data task, such as name, number, assigned to, priority, and state. |
| Related lists | |
| Goals | Details of the goals associated with the metric, such as name, state, category, start date, end date, owner, and status. To add a new goal, click **Add**. |
| Metric data | Details of the metric data such as start date, end date, value, collector metric data, collection frequency, and type.<br><br>Start date: The start date is the date the data collection begins.<br><br>End date: The end date is the end of the period date that determines the interval for which the score is calculated. The end date depends on the frequency of the metric definition. The end date is used for tracking the scores. Every score is time-dependent and it has a reference to the interval end date.<br><br>Collection frequency: The options in the collection frequency field are:<br>◦ Daily: Score that gets created for each day.<br>◦ Weekly: Score that gets created by the end of the week date (Sunday). Monday is the start of the week and Sunday is the end of the week.<br>◦ Monthly: Score that gets created by the end of the month.<br>◦ Quarterly: Score that gets created by the end of the quarter. For example, Q1 ends on March 31, Q2 ends on June 30, Q3 ends on September 30, and Q4 ends on December 31 in a year.<br>◦ Semi-annually: Score that gets created by the end of the 6-month period. The |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | end date for the semester is June 30 and December 31 in a year.<br>◦ Annually: Score that gets created by the end of the year. The end date for the year is December 31. |
| Targets | Details of the targets associated with the metric, such as name, state, owner, start date, end date, type, and measure. To add a new target, click **Add**. |
| Citations | Details of the citations, such as reference, name, authority document, description, and compliance score percentage (%). To add a new citation, click **Add**. |

4. To save the metric, click **Save**.
5. To delete the metric definition, click **Delete**.
6. To execute the metric, click **Execute**.
   A metric data score is created if it doesn't exist for the current interval. Re-executing a metric or a metric definition for the current interval only updates the score.
7. To visually explore the 360° relationship view of the metric definition, click **360° view**.

### Create a threshold for a metric definition

Evaluate the performance of your quantitative metric definition by defining threshold for your metric definitions.

#### Before you begin
Role required: admin

#### About this task
After you create a metric definition, you can define threshold limits for a metric and a metric definition to determine the performance of the metric. When the threshold value is breached or crossed, the system notifies the relevant owners. For example, you can create a metric definition to monitor employee attrition and define your target value for the metric, the amber threshold value and the red threshold value for a specified period. Now, consider that you defined your threshold value as 5, and your amber value as 8, and your red value as 10. This means that when there is an attrition of 8 people, the system will notify you about the metric performance as Amber. If your attrition reaches 10, the system will notify you about the metric performance as Red. This notification will enable you to take appropriate actions. You can create more than one threshold for a metric. If a threshold is defined before the metric is created, then the metrics inherit the rules of the threshold. You can create thresholds for all types of metric definitions. In this procedure, automated metric definition is used as an example.

If the threshold is created after the metric definition is created, you can copy the thresholds to the metrics.

#### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Metrics** > **Metrics**.
2. Select and open the metric for which you want to define the threshold.
3. Select the Thresholds related list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select **New**.
5. On the form, fill in the fields.

**Metric Definition Threshold form**

| Field | Description |
|---|---|
| Threshold type | Type of threshold. The choices are the following.<br>◦ Static: A static threshold for a metric or a metric definition refers to a fixed value used as a limit for tracking a metric.<br>◦ Dynamic: Dynamic thresholds are specified in percentages. This means that the percentage variance is calculated based on two factors: direction and the previous data<br>For more information, see .Thresholds in Integrated Risk Management |
| Amber threshold | Percentage value that signifies moderate change in the variance of target value. |
| Valid from | Date the data is valid from. |
| Target value | Previous data against which the percentage variance is compared. |
| Red threshold | Percentage value that signifies critical change in the variance of target value. |
| Valid until | Date the data is valid until. |

6. Select **Submit**.
7. To copy the thresholds to the metrics, select **Copy threshold**.

## Using GRC: Metrics to provide data

Using the GRC: Metrics application you can track your business goals, define your key risk indicators (KRIs) and key performance indicators (KPIs), and generate reports for the management to provide insights into the progress.

### Provide data for a metric data task

Use the metric data task to provide data for a manual metric.

#### Before you begin

Role required: sn_grc_metric.user, sn_risk.reader and sn_compliance.reader

#### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Metrics** > **My metric data tasks**.
2. Open the task for which you want to provide the data.
3. Click **Move to In Progress**.
4. On the Metric information form, under the Metric input section, fill in the following fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Metric data | Value for the metric. This field appears only when **Quantitative** is selected in the **Category** field in the metric form. |
| Unit | Unit of the data. For example, US gallon.<br>**Note:** You can provide the data in any unit and it gets converted to the reporting unit specified in the metric definition. |
| Response | Response for the metric. This field appears only when **Qualitative** is selected in the **Category** field in the metric form. |
| I certify and acknowledge that the response I have submitted is accurate. | Option to certify data accuracy. |
| Additional comments (Customer visible) | Additional information for the metric data. |

5. Select **Save**.
6. To provide evidence or supporting information, in the Related documents, related list, select **New**.
7. On the Related Document form, fill in the fields.

**Related Document form**

| Field | Description |
|---|---|
| Name | Provide a name for the supporting information. |
| Url | Select the lock icon to add a supporting URL. |
| Metric data task | This field is automatically set to the name of the metric data task for which you are providing information. |

8. Select **Submit**.

### Provide responses for multiple metrics

Use the metric tasks module to provide responses for multiple metrics in an easy-to-use format.

#### Before you begin

Role required: admin

#### About this task

As a data owner, you have to provide data or responses for multiple metric data tasks. The data that you provide comes from multiple sources and there can be multiple data owners. In such a scenario, it's hard to maintain the audit trail for data input. The metric tasks module enables you to provide data for multiple metric data tasks. Use the filters to select the metric

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

group for which you want to provide data. You can view the responses that you've entered, submitted, and also if the dates for data or for response submission are overdue. You can only provide metric data responses for tasks that aren't in the Closed state.

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace**.
2. Select the Metric data table icon (  )
3. From the Metric group list, select the metric group for which you want to provide data.

   Only those Groups which have open metric data tasks appear in the filter.
4. Double-click the cell for the entity in which you want to provide data.
5. Select the **I certify and acknowledge that the response I have submitted is accurate** option.
6. Select **Save**.
   Perform this step for each cell for which you want to provide data. You can scroll the cells to provide responses for all the tasks.
7. Select the tasks for which you want to submit the responses.

| Operating system | Keys |
|---|---|
| If you're a **macOS** user | Press the Command key and then click the cell to select. |
| If you're a **Windows** user | Press the Control key and then click to select the cell in focus. |

8. To provide any evidence for the data that you've entered, select the **Attachments and links** tab on the Contextual side panel and add the links and attachments as required.
9. Select **Submit**.

## Override metric data task response

As a metrics manager, if you think that the response provided for a quantitative metric must be modified, you can edit the data and provide a justification for the modification.

### Before you begin

Role required: sn_grc_metric.admin, sn_risk.admin, and sn_compliance.admin

### Procedure

1. Navigate to **All** > **Risk** > **Risk Workspace** > **Metrics** > **Metric data tasks**.
2. Open the task for which you want to edit the data.
3. Under the Metric input section, select the **Override Response** option.
4. In the **Overridden response** field, provide the new response.
5. In the **Justification** field, provide a justification for overriding the previous data.
6. In the **Additional comments** field, provide any additional comments that you have.
7. Select **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Override metric data

If the metric data provided by the data owner is inaccurate, then you can modify or override the metric data provided by the data owner.

**Before you begin**
Role required: sn_grc_metric.admin, sn_risk.admin, and sn_compliance.admin

**About this task**
After a metric data task is closed, the risk administrator can modify the metric data as needed. The risk administrator must provide a valid justification for modifying the data.

**Procedure**

1. Navigate to **All** > **Risk** > **Risk Workspace** > **List** > **Metrics** > **My metric data tasks**.
2. Open the record you want to modify.
3. On the Metric information form, under the Metric input section, select the **Override Metric Data** option.
4. In the **Overridden metric data** field, provide a new value.
5. In the **Justification** field, provide a valid justification for overriding the data.
6. In the **Additional comments** field, provide additional comments, if any.
7. Select **Save**.

**Result**
The metric data task value is overridden and the same value is updated in the metric data.

## GRC: Metrics reference

Several properties, tables, and roles are installed with the GRC: Metrics application.

### Components installed with the GRC: Metrics application

When the Risk Management application is activated, the GRC: Metrics application is automatically installed. The GRC: Metrics application adds roles that are listed here.

## Roles installed

The following roles are installed with the GRC: Metrics application.

**Roles installed with the GRC: Metrics application**

| Role | Description | Contains |
|---|---|---|
| sn_grc_metric.admin | This role serves as the Administrator within the application, and contains the responsibilities of the Metric Manager role. The role possesses the ability to override metric data results in metric data tasks and has the authority to delete metric definitions and metrics. Typically, this role is assigned to individuals holding positions as product | sn_grc_metric.manager, schedule_admin |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed with the GRC: Metrics application (continued)**

| Role | Description | Contains |
|---|---|---|
| | owners or application administrators. | |
| sn_grc_metric.manager | This role possesses the ability read, create, and update metric definitions and metrics. It is primarily assigned to risk managers, compliance managers, or business managers, who require the authority to define metrics within their respective areas of responsibility. | sn_grc_metric.user |
| sn_grc_metric.reader | This role is restricted to read-only access. It does not possess the privileges to create, edit, or update any metric definitions or metrics. However, as a metric reader, this role is authorized to review and approve metric data tasks where they have been designated as an approver. This role can be assigned to managers and executives if they want to access dashboards with metrics data to monitor the performance of the metrics. | None |
| sn_grc_metric.user | This role is primarily assigned to data owners, enabling them to respond to manual metric data entry tasks. Typically, these users are from the business and hold ownership responsibilities within the organization. | sn_grc.reader, sn_grc_metric.reader |
| sn_grc_metric.developer | Users with this role possess the privilege to write and edit the script for data collection automated metric definition. | None |

## Analytics and reporting solutions for Risk Management

Analytics and Reporting Solutions contain preconfigured dashboards. These dashboards contain actionable data visualizations that help you improve your business processes and practices.

This Analytics and Reporting Solution is available on the ServiceNow Store.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Request apps on the Store

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

Use the Platform Analytics widgets on the dashboard to visualize data over time, analyze your business processes, and identify areas of improvement. With Platform Analytics Solutions, you can get value from Performance Analytics for your application with minimal setup. You can always create your own objects as well.

**Important:** Set up and test Platform Analytics Solutions on a non-production instance before enabling them in production.

To enable the Analytics and Reporting solution for GRC: Risk Management, perform these steps.

1. Visit the ServiceNow Store and obtain an entitlement to the Performance Analytics - GRC: Risk Management application and associated applications. See Install a ServiceNow Product on the ServiceNow Store.
2. On the instance, navigate to **System Applications** > **All Applications** > **All**.
3. Locate and install the Performance Analytics - GRC: Risk Management application.

The following reports and dashboards are available in the Risk Management application.

## Operational risk heatmap for Advanced Risk Assessment in the Risk Workspace

As an operational risk manager, you can configure and manage your risk heatmaps in the Risk Workspace.

A risk heatmap is a data visualization tool that is used for communicating the specific risks that threaten an organization. Heatmaps are considered a critical component of enterprise risk management because it helps to identify risks that need more attention. In the Risk Workspace, you can configure your Advanced risk assessment heatmaps using the UI Builder. The heatmaps provide detailed information about your inherent and residual risks. The axes of the heatmaps can be configured in the inherent risk and residual risk configurations. To see how you can configure the axes details for the heatmap, see Configure an inherent assessment and Configure a residual assessment.

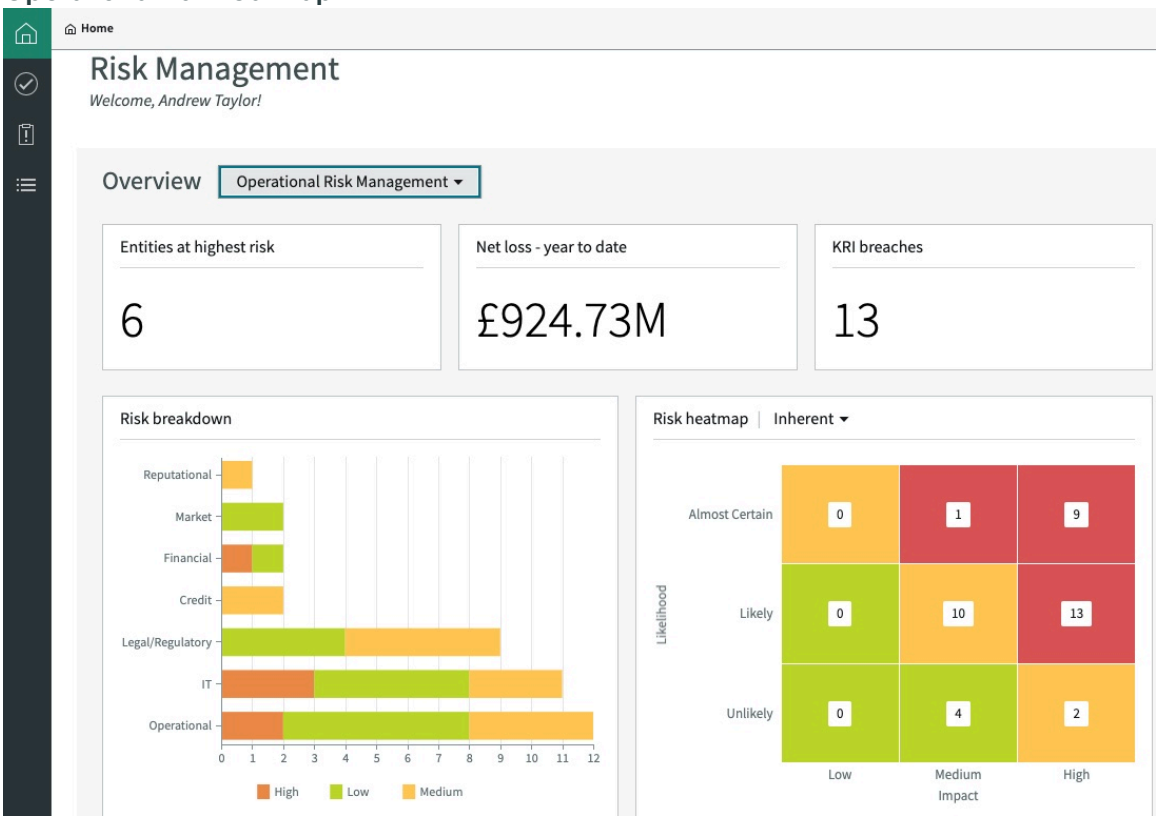
To view the operational risk heatmaps, ensure the following:

- Activate the **GRC: Risk Management workspace** (com.sn_risk_workspace) plugin.
- Activate the **GRC: Advanced Risk** (com.sn_risk_advanced) plugin.
- Enable the *Migrate to Advanced Risk Assessments* property.

In the **Summary** field, you can select the risk assessment methodology for which you want to view the heatmap. When you click any tile of the heatmap, you can view all the risks and their scores assessed for that particular risk assessment methodology. You can view the risk response strategy selected for those risks. If you want to define colors for your heatmaps, you can define the colors according to your preferences. For more information, see Create risk color styles.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Operational risk heatmap




To add or configure the heatmap in other pages or workspaces, see the Risk Heatmap Documentation [KB0994328] article in the Now Support Knowledge Base

## Risk heatmap for classic risk assessment

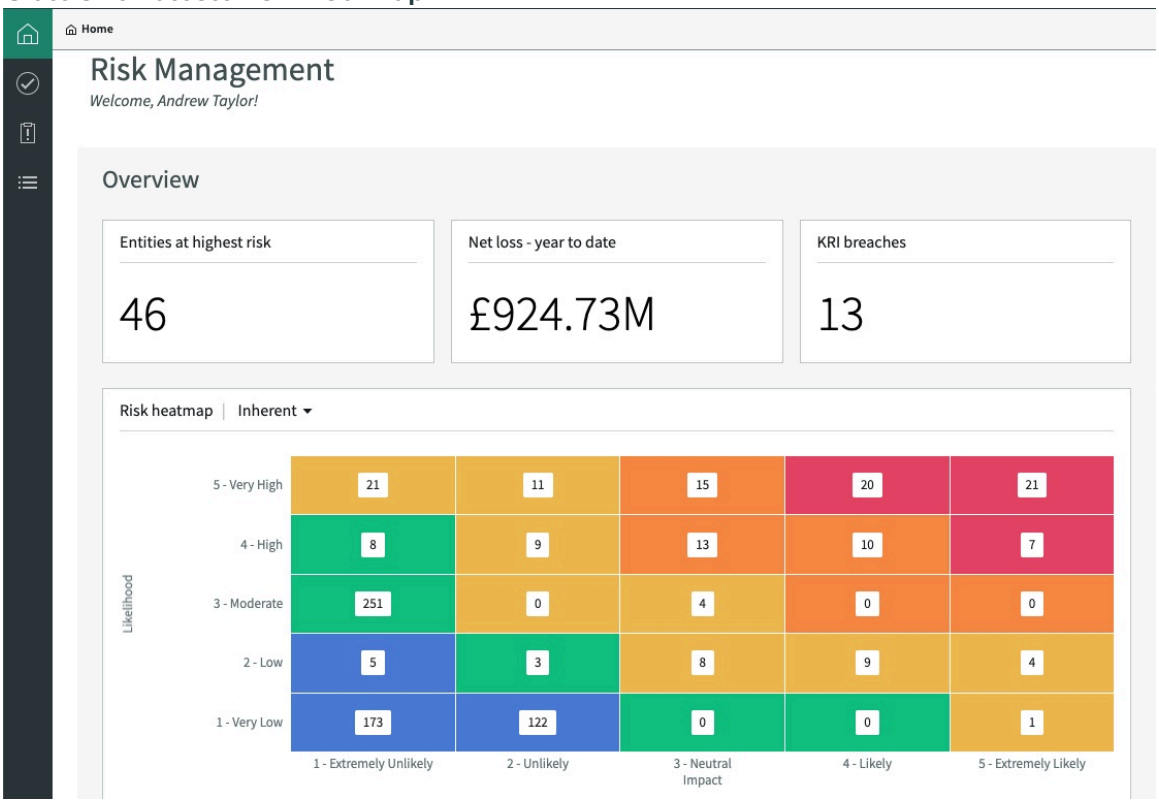
As an operational risk manager, if you opt to use the classic risk assessment to assess the risks in your organization, you can view the risk heatmap to get an overview of the risk posture for your organization.

A risk heatmap is a data visualization tool that is used for communicating the specific risks that threaten an organization. A risk heatmap is considered a critical component of enterprise risk management because it helps to identify risks that need more attention.

To view the operational risk heatmaps, ensure that you activate the GRC Risk Management (sn_risk) plugin. When you click any tile of the heatmap, you can view the risk records and see the entity, the risk statement, the owning group, the owner and the calculated scores.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Classic risk assessment heatmap



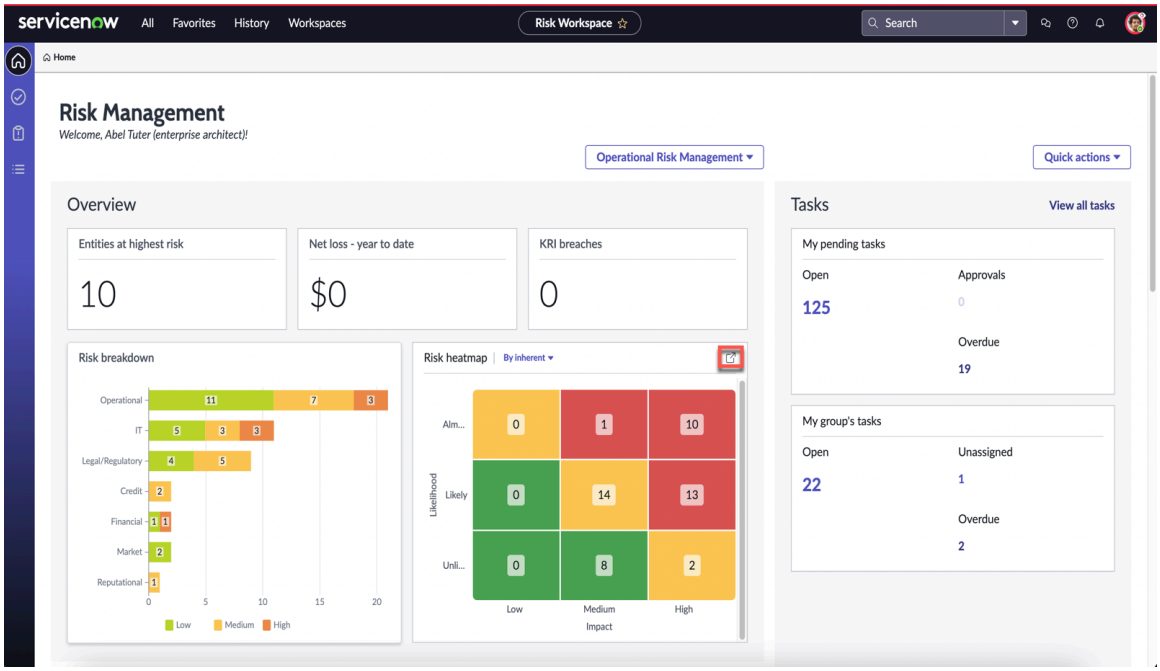

## Risk heatmap workbench

As an operational risk manager, you can visualize the risk details and better understand the risk posture of your entity by using the risk heatmap workbench in the Advanced Risk application.

## Overview of the heatmap workbench

A risk heatmap is a graphical representation of your risk data where the individual values that are contained in a matrix are represented in colors that denote a meaning. You can use risk heatmaps to see your risk assessment results in a convenient, visually attractive, and succinct format. Starting in version 14.0, you can launch the risk heatmap workbench with the launch workbench icon ( ).

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

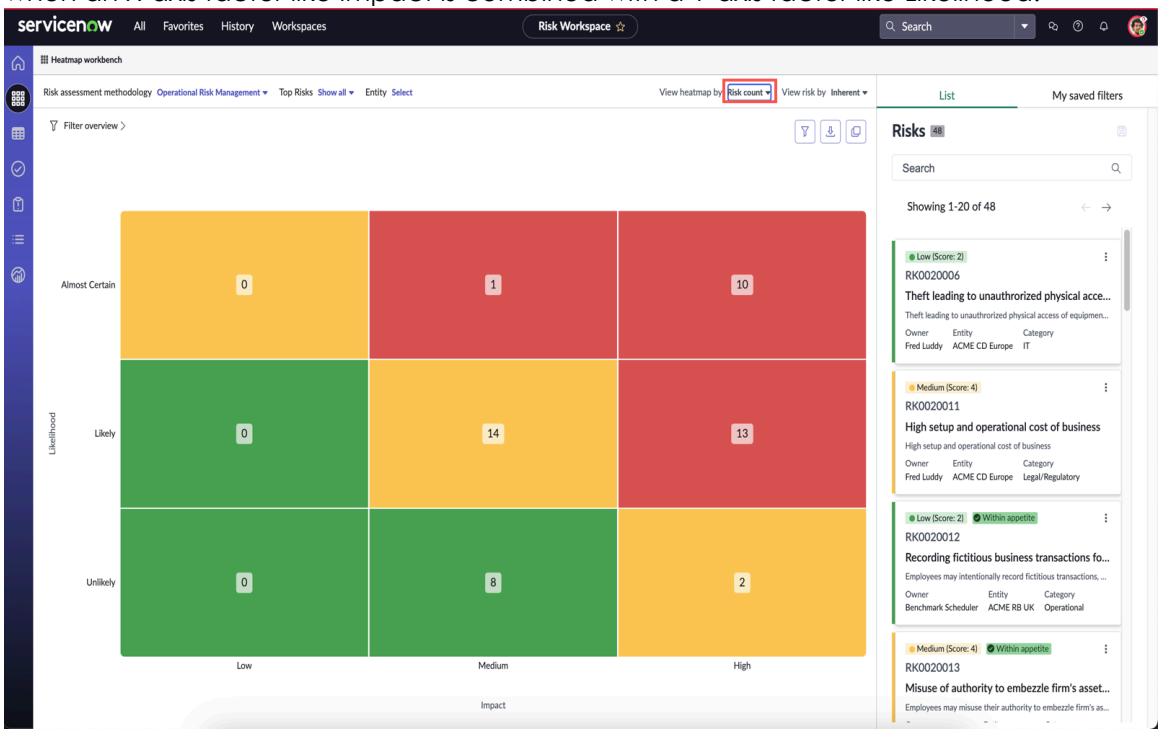



## Features of the heatmap workbench

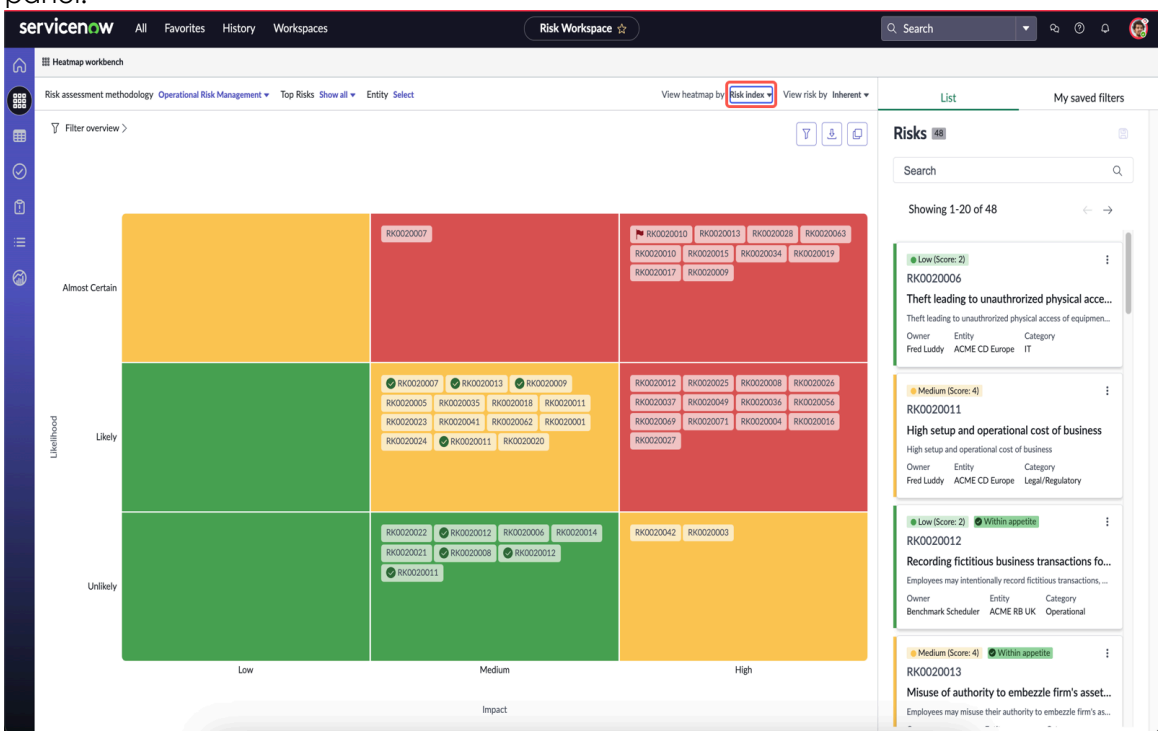
By using the risk heatmap workbench, you can view the following aspects for risks:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Risk count: Shows the number of risks that are in each cell on a heatmap such as when an X-axis factor like Impact is combined with a Y-axis factor like Likelihood.

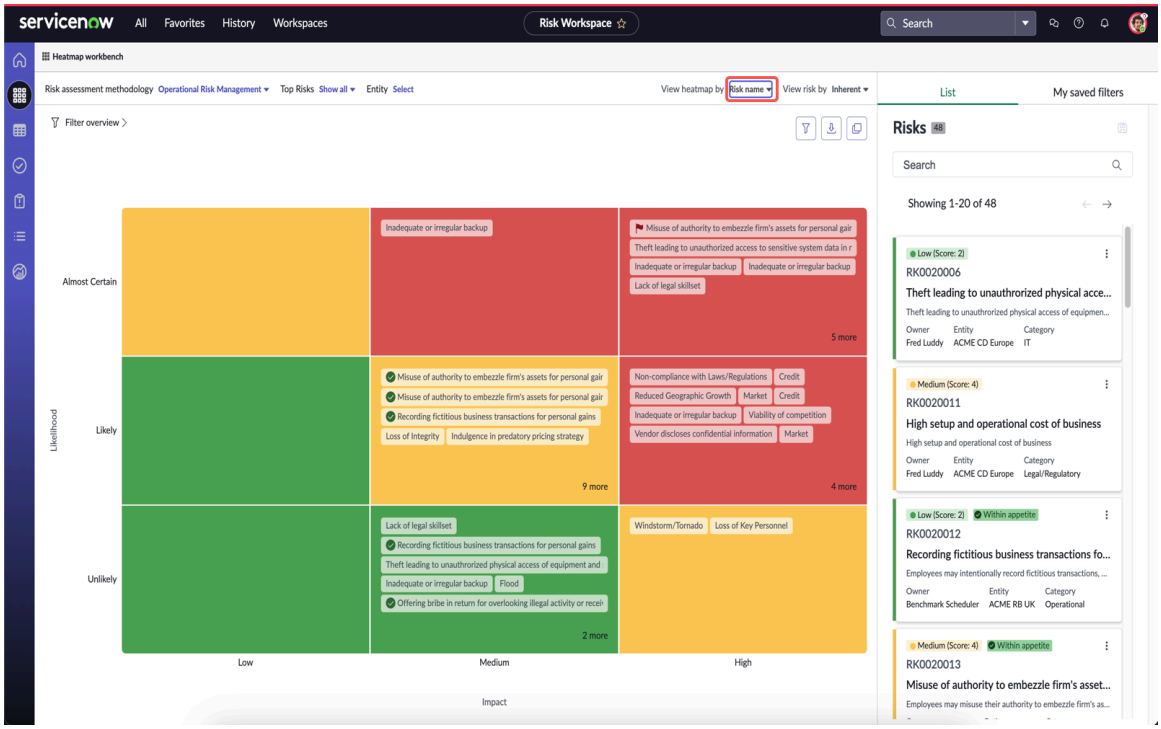



- Risk index: Shows the risk IDs in each cell and the details of each risk on the contextual side panel.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Risk name: Shows the names of all the risks in each cell.




- Top Risks: Shows the top risks on the heatmap workbench. For example, if you select 10 from the Top Risks filter selection list, you can see all the top 10 risks that are associated with the selected Risk Assessment Methodology (RAM) on the heatmap.
- Entity: Shows the risks that are associated with the specific entities and their downstream entities on the heatmap workbench. You can filter the risks that are associated with the specific entities that are defined in the RAM.

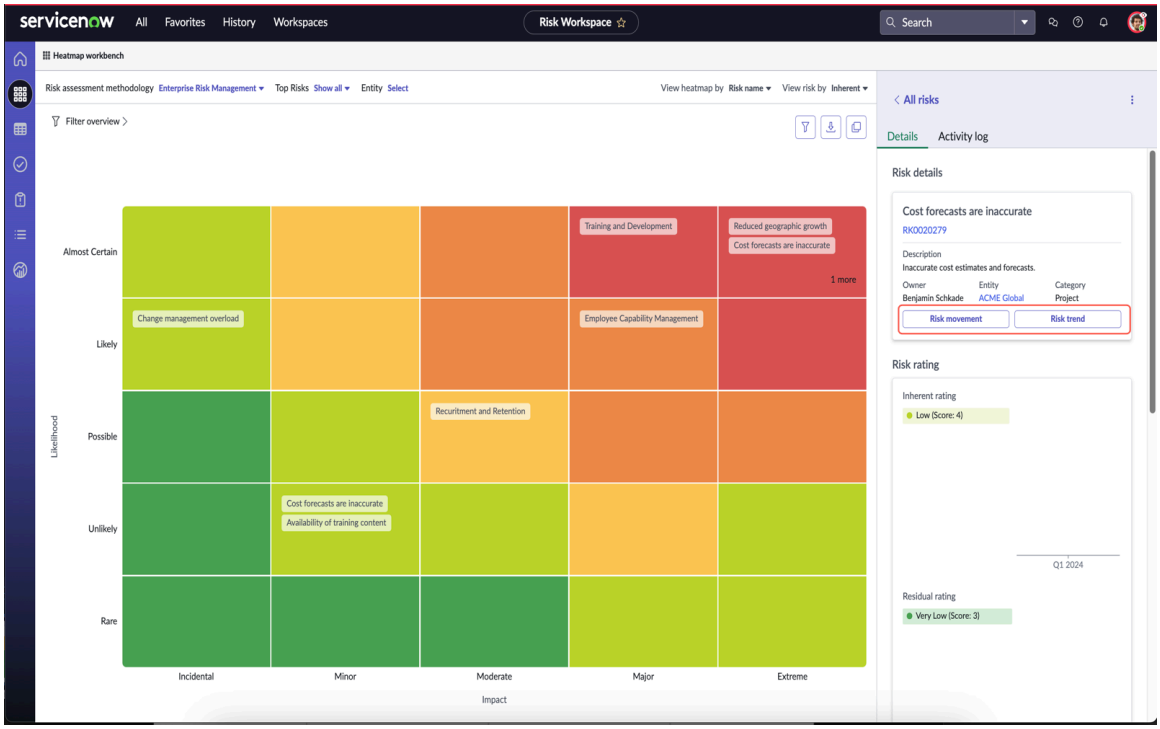
By pointing to each risk, you can quickly get details about the risk. For example, you can see who the risk owner is, the entity to which the risk belongs, and the category of the risk. The contextual side panel shows 20 entries at a time on a page. You can configure the total number of entries that you want to see. You can either view all the risks as cards or select a single risk and view its details. After you select a risk from the heatmap cell, you can see the details of that risk on the side panel. For example, you can see the risk rating, the risk response, the risk tracking, and the risk hierarchy. The activity log captures all the activities that are performed on a risk. If you click the more actions icon ⋮, you can see the following options:

- **Open**: Provides the risk record.
- **360° view**: Provides an overview of the associated entities, controls, risk statements, risk assessments, and risk response tasks.
- **View assessment**: Provides an assessment summary of the risk.

## Reporting in the heatmap workbench

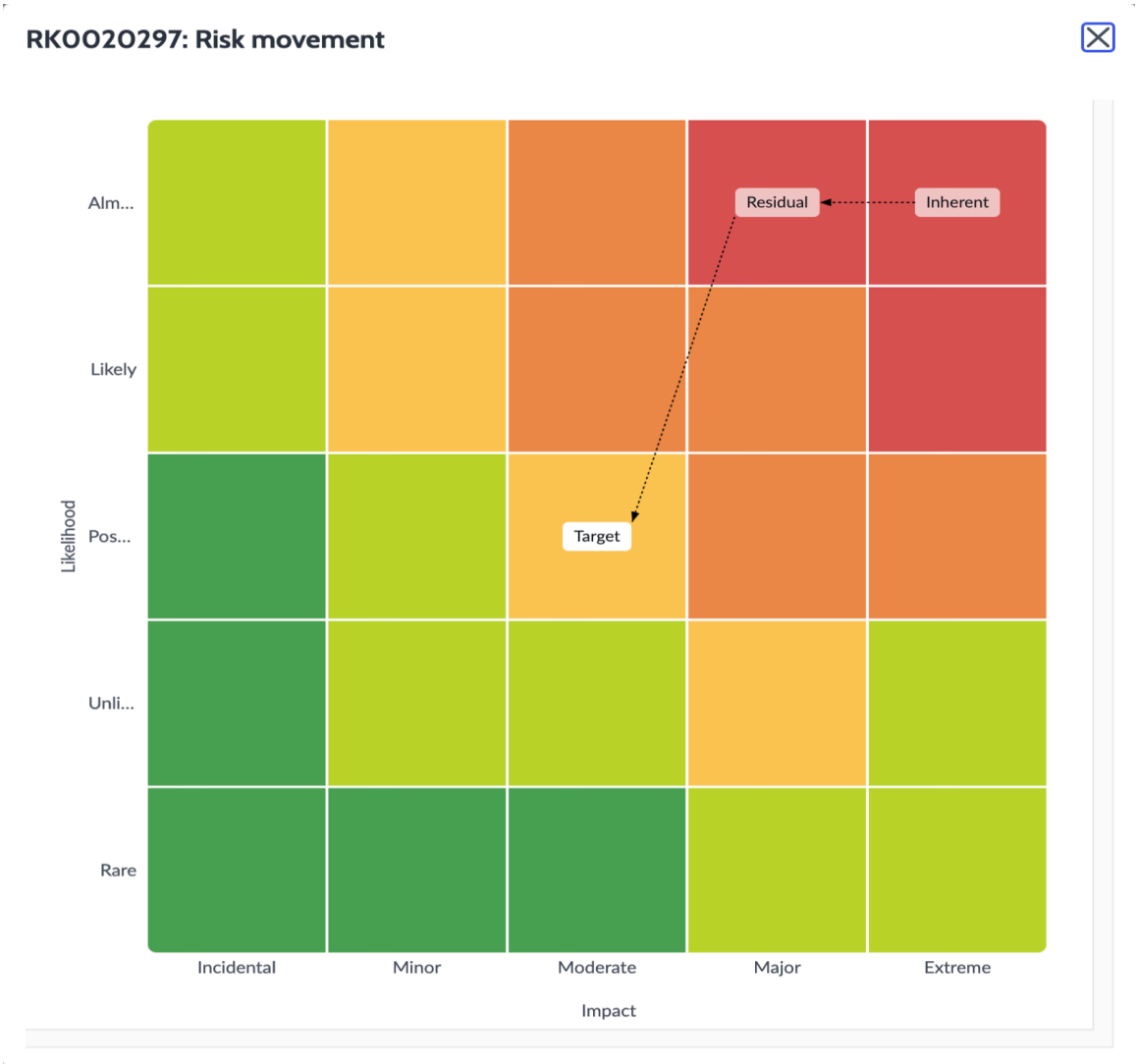
The heatmap workbench is the primary tool that you use for risk reporting and analysis. By looking at the Risk movement and Risk trend, you can visualize your organization's risk profile and share that information with your stakeholders.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




You can view the risk movement from inherent (risk level without controls or mitigating actions), to residual risk (leftover risk after the implementation of controls), finally to target risk (risk level that you want to achieve in future) on the heatmap workbench. This information helps you to analyze the assigned controls to mitigate if the risks are effective or not. The risk movement is available only for RAMs where the residual risk has the same factors as an inherent risk.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




You can view the risk score movement across multiple assessments on the heatmap workbench. The risk trend shows how the risk has changed and analyzes how you have been managing the risk. The risk trend is available for the last five risk assessments. You can also disable the trend line on the heatmap for a clear and less cluttered view.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

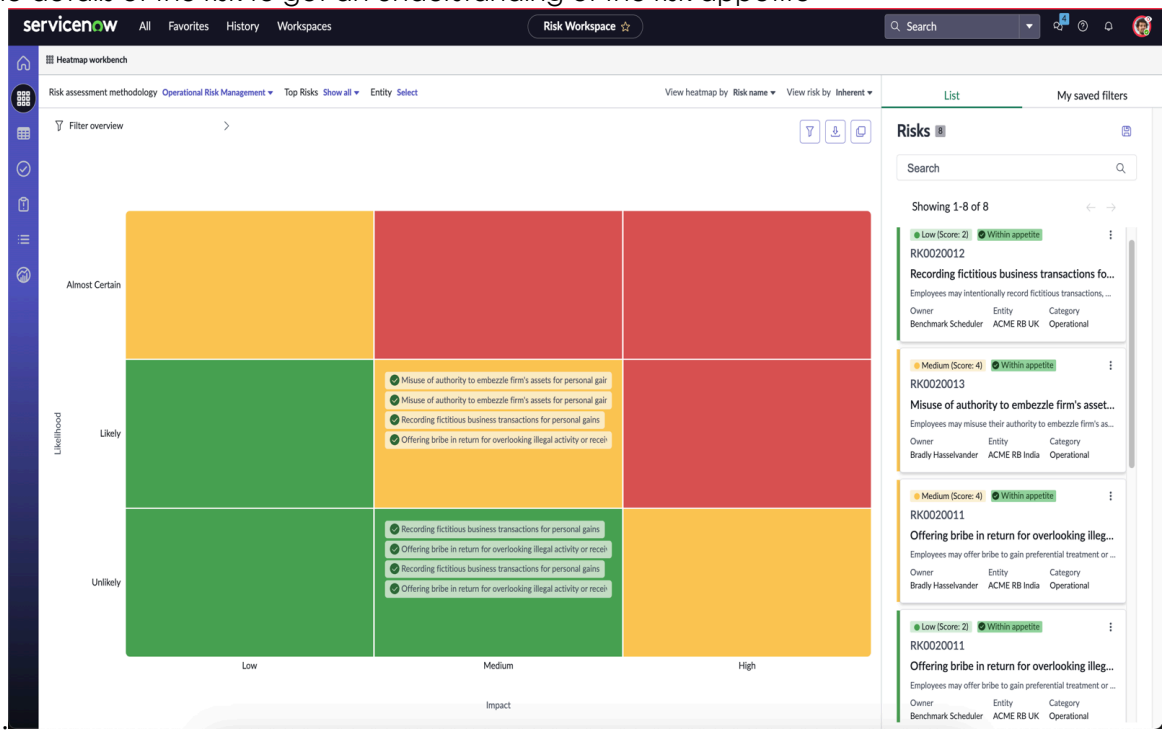



## Risk appetite in the heatmap workbench

You can view the status of the risk appetite on the heatmap workbench. The risk appetite trend is also available on the heatmap. You can also

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

see the details of the risk to get an understanding of the risk appetite status.




## Filtering in the heatmap workbench

You can filter the data that you see on the heatmap workbench. For example, let's say that you see 40 entries on the heatmap and you'd like to filter those risks where the entity is ACME Global. You can use the condition builder and apply your filters. After the filters are applied, the heatmap is refreshed and displays the data based on the filter conditions that you have applied. For more information on how to filter the data, see Filter data in the risk heatmap workbench. The ability to filter is only available in the workbench view. You can save the frequently used filters in the My saved filters section.

## Downloading and copying in the heatmap workbench

You can download or copy the risk heatmap information to include in reports or share with relevant stakeholders as needed. The download icon enables you to download the heatmap as an image. The copy icon enables you to copy the heatmap information in your clipboard. You can then paste it into emails, reports, presentations, or other documents to share the visual data representation as needed.

## Searching in the heatmap workbench

As a risk user, while looking for a particular risk, you can quickly search a risk by the name, owner, or any of the other information that is shown in the card. You can also filter the data by searching the risks. In the contextual side panel, you can enter your keyword in the search field and the filtered results are visible.

**Note:** The search feature considers the risk name, risk description, and fields that are shown in the card. For example, if you search for the word Operational, then all risks that have the word operational will appear in the search result.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

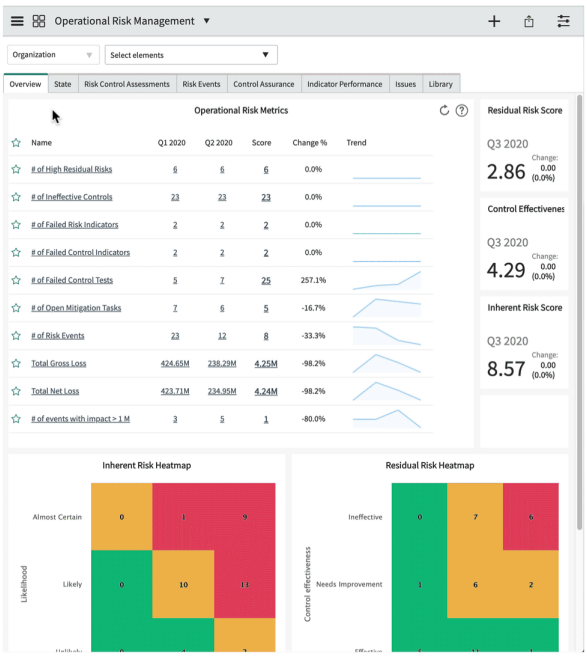
## Immersive view of the heatmap workbench

With the immersive view of the heatmap, you can view the expanded form of the heatmap where the X-axis and the Y-axis values are highlighted. The benefit of this view is that if you have too much information in one zone, you can focus on that zone and analyze each risk. The pagination enables you to see all records. You can point to a risk to quickly understand more details about the risk. You can also view the different values of both the axes by clicking the value. For example, let's say that in the heatmap, the X-axis has the values low, medium, and high and the Y-axis has the values unlikely, likely, and almost certain. You can click any value in both the axes to see the risks for that combination.

## Operational Risk Management dashboard

The Operational Risk Management dashboard enables an entity owner, with the role sn_risk.user, to view the complete risk posture for the enterprise in a single consolidated report. This dashboard makes it easy to analyze the risk posture efficiently and take necessary corrective actions to ensure that there are no losses.

### Operational risk dashboard




## End user and roles

| End user and goal | Required role | Benefits |
|---|---|---|
| Risk user: Operational risk captures business continuity plans, environmental risk, process systems, operations risk, and people-related risks. | sn_risk.user | • Improves the reliability of business operations.<br>• Improves the effectiveness of risk management operations.<br>• Strengthens the decision-making process.<br>• Reduces losses caused by unidentified or poorly-identified risks. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| End user and goal | Required role | Benefits |
| --- | --- | --- |
| | | • Detects unlawful activities early.<br>• Lowers compliance costs.<br>• Reduces potential damage from future risks. |

Operational risk is the risk of loss that is incurred from inadequate or inefficient internal processes, people, and systems, or from external events. Operational risk captures the following to provide the complete risk posture of an organization:

- Risk identification and assessment
- Risk events data
- Identifying and assessing internal controls
- Monitoring and reporting of risks

## Indicators

Indicators define a performance measurement taken at regular intervals of a business service, an activity, or organizational behavior. These performance measurements result in a series of indicator scores over time. To view this dashboard, users must have Advanced Risk and Policy and Compliance Management plugins activated

To view the list of all indicators for all the associated plugins, see the following:

- GRC Advanced Risk plugin indicators
- GRC Policy and Compliance Management plugin indicators
- GRC Audit Management plugin indicators
- GRC Risk Management plugin Performance Analytics indicators
- GRC Profiles plugin indicators

**Note:** There are two jobs that you must run to collect data for this dashboard.

- **Daily Data Collector job**: This job is used to collect data for the Indicators. This jobs runs daily. To run this job, you must fill the **Run as** field with an appropriate value. This job is preconfigured.
- **Historical Data Collector job**: This job is used to collect data over a period of time. This job is generally preconfigured with the demo data. Therefore, if you enable demo data, while activating the plugin, then you can view this job. To run this job, you must fill the **Run as** field with an appropriate value.

## Breakdowns

Organization (Entity)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Reports

| Title | Type | Description |
|---|---|---|
| Risk Response by Residual Risk Rating |  Heatmap | Heatmap which shows the number of different risk response tasks for each residual risks. |
| Controls by owner | Horizontal bar | Controls distributed on the basis of their owners. |
| Risks by owner | Horizontal bar | Risks distributed on the basis of their owners. |
| Inherent risks by category | Horizontal bar | Number of risk assessments with different inherent risk levels grouped by risk statement categories such as credit, market and so on. |
| Residual risks by category | Horizontal bar | Number of risk assessments with different residual risk levels grouped by risk statement categories such as credit, market, and so on. |
| Control Test | List | List of all controls. |
| Control Indicators | List | Indicators associated with each control. |
| Risk Indicators | List | Indicators associated with each risk. |
| Controls by classifications | Pie chart | Controls distribution on the basis of its classification like preventive or detective. |
| Controls by attestation frequency | Pie chart | Controls distributed on the basis of attestation frequency. |
| Risks by category | Pie chart | Risk distribution on the basis of category. |
| Overdue issues | Single score | Number of open issues that are past their planned end date. |
| Active risk events | Single score | Number of active risk events. |
| Pending attestations | Single score | Number of controls awaiting attestation. |
| Overdue assessment task | Single score | Number of risk assessments with the substate as Overdue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Title | Type | Description |
|---|---|---|
| Upcoming acceptance expiry | Single score | Number of risk acceptance tasks with acceptance end date in next 10 days. |
| Open mitigation tasks | Single score | Number of open mitigation tasks. |
| Open indicator tasks | Single score | Number of open indicator tasks. |
| Overdue control tests | Single score | Number of open control tests that are past their planned end date. |

### GRC Advanced Risk plugin indicators

The GRC Advanced Risk plugin contains various indicators.

The Advanced Risk plugin includes the following indicators:

# of high residual risks
: Number of high residual risks per quarter.

# of ineffective controls
: Number of ineffective controls per quarter.

Maximum of maximum calculated ALE for this quarter
: Maximum of maximum calculated ALE for this quarter.

Maximum of maximum acceptable loss expectancy for this quarter
: All active risk statements updated within the current quarter and calculates the average of maximum_acceptable_loss_expectancy

Number of open mitigation tasks
: Number of risk mitigation tasks in open state in this quarter.

# of risk events
: Number of risk events that were reported in this quarter.

Total gross loss
: Total gross loss from financial risk events per quarter.

Total net loss
: Total net loss from financial risk events per quarter.

Active Events
: Number of active risk events per quarter.

# of events with impact > 1 M
: Number of risk events with financial impact greater than one million USD.

Average residual risk
: Average residual risk score per quarter.

Average control effectiveness
: Average control effectiveness per quarter.

Average Inherent Risk
: Average inherent risk score per quarter.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Risk Assessments (Open)

Open risk assessments.

Issues (created this quarter)

Issues created per quarter.

Indicator task (created this quarter)

Indicator tasks per quarter.

Control tests (created this quarter)

Control tests per quarter.

Risk assessments in Monitor state

Risk assessments in monitor state.

Non-financial risk events

Number of non-financial risk events per quarter.

Total potential loss

Total potential loss from financial risk events per quarter.

Total expected loss

Total expected loss from financial risk events per quarter.

# of events with high non-financial impact

Number of risk events with high non financial impact per quarter.

Average gross loss per event

Average of the gross loss incurred for each active risk event.

Average net loss per event

Average net loss per event. Net loss = Gross loss minus recovery loss.

Average recovery made per loss event

Average recovery made per loss event per quarter.

Average additional cost per event

Average additional cost per financial risk event per quarter.

Annual Loss Expectancy

Average ALE monthly is measured monthly as unit.

Number of entity

Number of entities which are in active state and updated during or before this quarter.

Near Miss

Number of near miss risk events per quarter.

Number of risk statements

Number of risk statement which are in active state and updated during or before this quarter.

Total control indicators

Number of control indicators running per quarter

High risks with failed indicators

Number of risks with high rating and failed indicators in the quarter.

Overdue indicator tasks

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Number of indicator tasks due in the quarter.

Percentage of risk indicators failed

Percentage of failed risk indicators.

Total Failed Indicators Quarterly

Number of failed indicators in the quarter.

High Risk with Failed Control

Number of High Risk with Failed Control Test

Total Risk Indicators

Number of risk indicators running per quarter.

# of ineffective controls

Number of ineffective controls per quarter.

# of failed risk indicators

Number of failed risk indicators per quarter.

# of Failed Control Tests

Number of failed control tests per quarter.

Failed Control Test Quarterly

Number of Failed Control Test Quarterly

By this quarter

Total number of remediation task that needs to be completed by this quarter.

Key Controls with Failed indicators

Key Controls with Failed indicators is measured quarterly

### GRC Audit Management plugin indicators

The GRC Audit Management plugin contains various indicators.

The Audit Management plugin includes the following indicators:

Key controls not tested

Number of key controls that are not tested.

Failed Controls

Number of controls whose control tests are ineffective.

Open Audit Issue

Number of open audit issues

Passed controls

Number of controls whose control tests are effective.

Ongoing Control Test

Number of Ongoing Control Tests

Failed control test quarterly

Number of failed control tests in a quarter.

New controls

Number of new controls.

### GRC Policy and Compliance Management plugin indicators

The GRC Policy and Compliance Management plugin contains various indicators.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Policy and Compliance Management plugin includes the following indicators:

# of failed control indicators
: Number of failed control indicators per quarter.

Controls (not retired)
: Number of non-retired controls.

Control not Attested
: Number of controls whose state is in draft or attest.

Orphan controls
: Number of controls without control objective

Mandated Controls
: Number of controls whose enforcement is mandatory.

Key Controls
: Number of key controls

Controls without Test Plans
: Number of controls without test plans.

Exempted controls
: Number of exempted controls.

Controls without KCI's
: Number of controls without indicators.

Active Controls
: Number of active controls.

### GRC Risk Management plugin Performance Analytics indicators

The GRC Risk Management plugin contains various Performance Analytics indicators.

The GRC: Risk Management plugin includes the following Performance Analytics indicators:

Risk without mitigating control
: Number of risks without mitigating control.

Active Risk
: Number of Active Risks

New risk
: Number of risks which are in draft state.

Risk without KRI's
: Number of Risk's without KRI's.

Orphan risks
: Number of risks without risk statement.

Risk not assessed
: Number of risks which are not assessed.

### GRC Profiles plugin indicators

The GRC Profiles plugin contains various indicators.

The GRC: Profiles plugin includes the following indicators:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Open remediation tasks

Number of open remediation tasks

Today

Number of issues closed today.

Today

Number of issues created today.

By this year

Total number of issues that need to be resolved by this year.

By this quarter

Total number of issues that needs to be resolved by this quarter.

By this month

Total number of issues that need to be resolved by this month.

All open issues

Number of open issues

All Unassigned Issues

Number of unassigned issues.

Remediation Task Aging Indicator

Remediation Task Age Distribution on the basis of state.

All Open Issues QoQ

All Open Issues Quarter to Quarter

Issues Aging Indicator

Issue Age Distribution on the basis of state.

By this week

Total number of issues that needs to be resolved by this week.

This quarter

Number of issues closed on this quarter.

New issues

Number of new issues

This month

Number of issues created this Month.

By today

Total number of remediation task that needs to be completed by today.

This week

Number of issues closed on this week.

This week

Number of issues created this week

By today

Total number of issues that need to be resolved by today.

This quarter

Number of issues created in this quarter.

By this year

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Total number of remediation tasks that need to be completed by this year.

By this month

Total number of remediation task that needs to be completed this month.

By this week

Total number of remediation tasks that needs to be completed by this week.

This month

Number of issues closed on this month

### Risk register in the Risk Workspace

The risk register contains the information about identified risks, results of risk analysis such as risk scores, and risk response plans. The risk register enables you to monitor and control the risks of your organization.

A risk register is a crucial risk analysis tool used in enterprise risk management. It is a record of information of identified risks. A risk register is used for regulatory compliance and keeps risk managers updated about the enterprise risks. It is important to regularly monitor risks and responses. A risk register simplifies this task by showing at a glance:

- Which risks exist?
- Which risks are the most threatening?
- How must the enterprise deal with those risks?
- Should some risks be accepted?
- What is the mitigation plan?

To view the Risk Register, navigate to **Risk Workspace** > **Risk assessments** > **Risk Register**

The components of the Risk Register are the following:

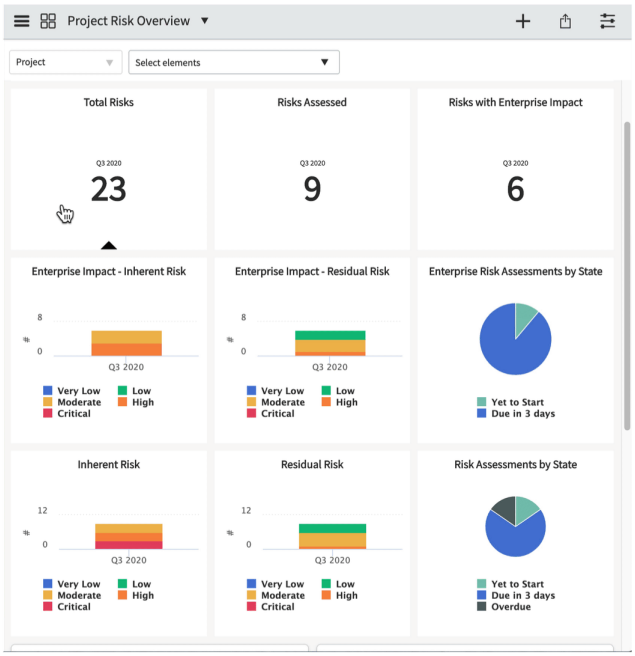
- Entities that are assessed for risks.
- The risk assessment methodology that is used for risk assessment.
- The assessor of the risk assessment
- The risk assessment scores for:
  - Inherent risks
  - Control effectiveness
  - Residual risk
- The risk responses for each risk.

## Project Risk Overview dashboard

The project risk dashboard is useful for project managers and the enterprise risk managers. Using this dashboard, the project managers and enterprise risk managers can view the risk performance and the overall risk posture. This dashboard helps risk managers to reduce the overall risks in an organization.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Project Risk Overview dashboard




## Required roles

- To edit the dashboard, users must have it_pps_admin or sn_risk.admin roles.
- To view the dashboard, users must have sn_risk.reader role or it_project_manager, or sn_ppm.read roles.
- To view the details of the records, users must have the sn_grc.business_user role.

## Use cases

For examples of how different people in your organization would use this dashboard, see these use cases.

| User | Dashboard use |
|---|---|
| Enterprise risk manager | The enterprise risk manager can view the different enterprise risks and understand how many risks are critical, high, moderate, low, and very low. This dashboard provides an understanding of the overall enterprise risk posture. |
| Project manager | The project manager can select the project for which they want to view the risks.<br>They can view the trend of the risks on a quarter-by-quarter basis, the number of risks assessed, the number of risks that affect the enterprise, and so on. The heatmap aggregates all the project risks that are assessed. It helps to keep a track of the bad risks and helps to manage them. This reduces the overall risk exposure for an organization. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Indicators

PPM-Total Risks

Count of all risks with a parent project.

PPM-Enterprise Risk Assessments

Count of all risk assessments with risk assessment methodology as Enterprise Assessment for Projects and the entity class as Project.

PPM- Project Risk Enterprise

Count of all risk assessments with risk assessment methodology as Project Risk Assessment and with table as risk.

PPM-Risks Assessed

Count of all risks with project risk assessment in the Monitor state.

PPM-Risks with Enterprise Impact

Count of all risks with enterprise risk assessment in the Monitor state.

## Breakdowns

- Project
- Project and Enterprise Risk Assessment States
- Qualitative Rating Criteria - Enterprise Inherent Assessment
- Qualitative Rating Criteria - Enterprise Residual Assessment
- Qualitative Rating Criteria - Project Inherent Assessment
- Qualitative Rating Criteria - Project Residual Assessment

## Reports

This dashboard displays the following reports:

| Title | Type | Description |
|---|---|---|
| Total risks |  Single score | Total number of project risks identified. |
| Risks assessed |  Single score | Total number of project risks assessed. |
| Risks with enterprise impact |  Single score | Total number of risks with enterprise impact. |
| Enterprise impact- inherent risk |  Bar graph | Number of inherent risks with enterprise impact. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Title | Type | Description |
|---|---|---|
| Enterprise impact- residual risk | Bar graph  | Number of residual risks with enterprise impact. |
| Enterprise risk assessments by state | Pie chart  | Number of enterprise risk assessments by states. |
| Inherent risk | Bar graph  | Number of inherent project risks. |
| Residual risk | Bar graph  | Number of residual project risks. |
| Risk assessment by state | Pie chart  | Number of project risk assessments by states. |
| Inherent risk by likelihood and impact | Heatmap  | Aggregation of all the inherent project risks and their impact. |
| Residual risk by likelihood and impact | Heatmap  | Aggregation of all the residual project risks and their impact. |

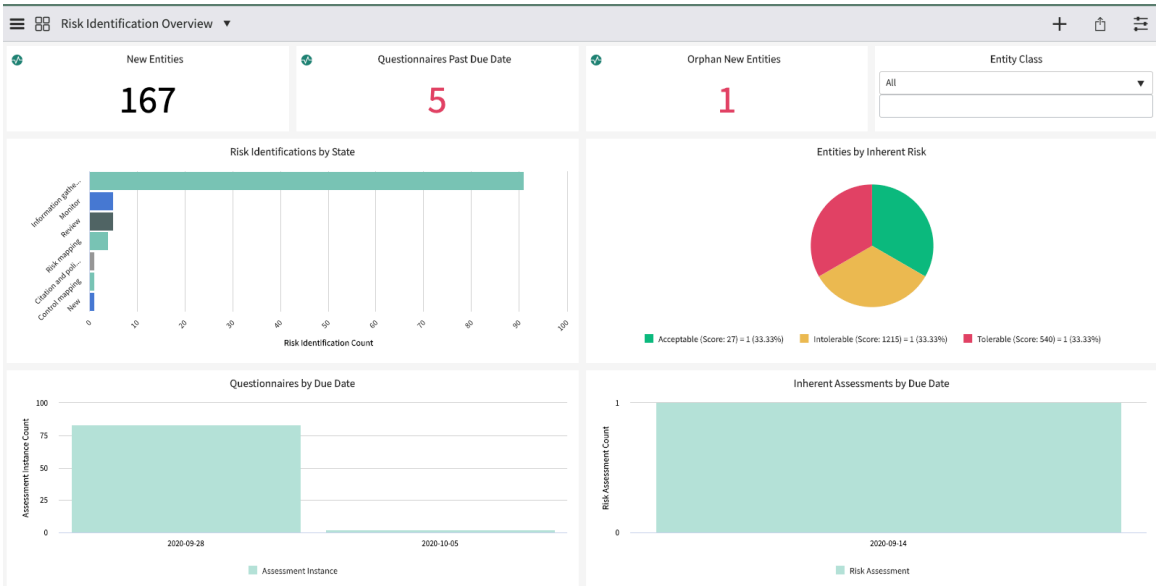
## Risk Identification Overview dashboard

The risk identification dashboard is useful for risk managers and helps them to keep a track of various records or objects which are in transit in the risk identification workflow.

This dashboard offers various insights for the users. These insights enable risk managers to decide the required action and helps them to prioritize the risk identification records that need attention. For example, if there are questionnaires past their due date, the risk managers may want to follow up with the person who was assigned the questionnaire.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Risk Identification Overview




## Reports

This dashboard displays the following reports:

| Title | Type | Description |
|---|---|---|
| New Entities |  Single score | The number of new entities created in GRC in the last week. This report notifies the risk manager of the new entities. The risk manager can map the risks and controls for the new entities and check if the risk identification workflow is initiated or not. |
| Questionnaires Past Due Date |  Single score | The number of questionnaires that have past their due date. This allows the risk manager to track the number of overdue questionnaires and take necessary actions. |
| Orphan New Entities |  Single score | The number of new entities created weekly that do not have an owner. Orphan entities have risks and controls with no one acting upon those risks. This report allows the risk manager to track entities for which an owner is missing and identify an owner to respond to the survey. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Title | Type | Description |
|---|---|---|
| Risk Identifications by State | Horizontal bar  | The number of risk identification records grouped by state such as:<br>• New<br>• Information gathering<br>• Control mapping<br>• Citations and Policies<br>• Risk Mapping<br>• Review<br>• Monitor |
| Entities by Inherent Risk | Pie chart  | The number of risk identifications grouped by inherent risk ratings. This report allows the risk manager to track risk identification based on inherent risk ratings and highlight the critical entities that need immediate attention. |
| Inherent Assessments by Due Date | Bar graph  | The number of upcoming inherent assessments assigned to a user based on the due date. This is a weekly report. |
| Questionnaires by Due Date | Bar graph  | The number of upcoming questionnaires assigned to a user based on the due dates. This is a weekly report. |

## Basel dashboard

The Basel dashboard is a medium to share the Basel reports with external regulators for Basel regulations. This dashboard is useful for banking and financial domains where it is compulsory to share the Basel reports.

As a business user, you can choose to enable or disable displaying this dashboard by configuring the *Show Basel attributes and properties* property under *Risk Event Properties*.

This dashboard has two tabs:

- LOB to Category Mapping reports:
  - Net loss by Business Line & Category (YTD)
  - Net loss by Business Line & Category (QTD)
  - Number of Events by Business Line & Category (YTD)
  - Number of Events by Business Line & Category (QTD)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

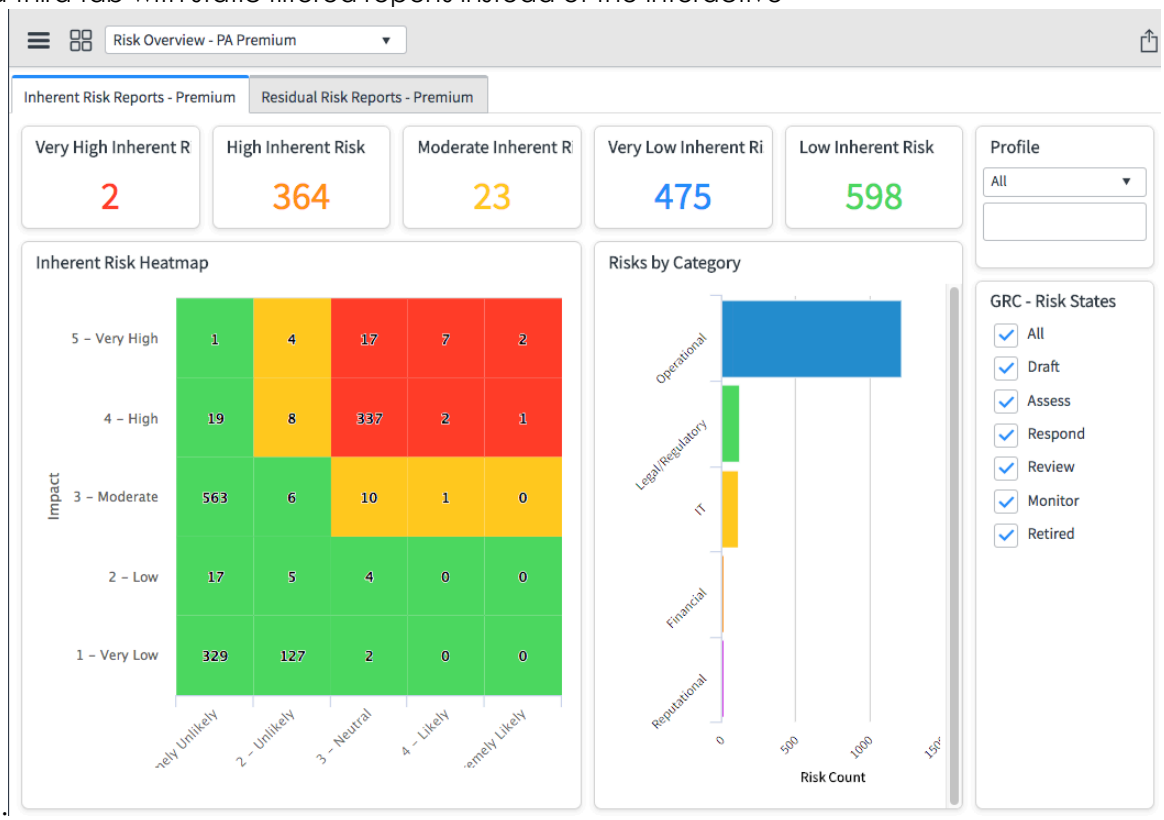
- Risk Events by Open & Closed State reports:
  - Open Risk Events by Basel Category
  - Closed Risk Events by Basel Category
  - Open Risk Events by Line of Business
  - Closed Risk Events by Line of Business

## GRC Risk Overview dashboard

The Risk Overview dashboard provides an executive view into the status and workflows of inherent and residual enterprise and IT risks. The user can drill down into risks by framework, response, and exception.

There are two versions of this dashboard. The Premium version utilizes interactive filters and requires the licensed version of Performance Analytics.

The Risk Overview dashboard has two views, one with inherent risk reports and one with residual risk reports. The Premium version of the dashboard, which uses interactive filters, is shown. The other version of the dashboard has a third tab with static filtered reports instead of the interactive filters.




## End users

| End user and goal | Required role |
|---|---|
| Audit Manager: Needs clear visibility into the overall state and volume of vulnerabilities within the organization. | sn_risk.manager |
| Audit Administrator: Needs to pinpoint areas of concern quickly | sn_risk.admin |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| End user and goal | Required role |
| --- | --- |
| Audit Analyst: Needs to quickly prioritize which risks/tasks to focus on based upon criticality to the organization. | sn_risk.user |

## Reports

The Risk Overview dashboard contains the following reports:

| Name | Type | Description |
| --- | --- | --- |
| High Inherent Risk | Single Score | Number of risks with High Inherent Risk status |
| High Residual Risk | Single Score | Number of risks with High Residual Risk status |
| Inherent Annual Loss Exposures | Box | Calculation of the inherent Annualized Loss Expectancy (ALE) |
| Inherent Risk | Bubble | Calculation of the inherent risk score from the likelihood and significance of a risk. |
| Inherent Risk Heatmap | Heatmap | Inherent risk heatmap providing total number of risks by very high risk, high risk, moderate risk, low risk and very low risk |
| Low Inherent Risk | Single Score | Displays the number (count) of low inherent risks. |
| Low Residual Risk | Single Score | Displays the number (count) of low residual risks. |
| Moderate Inherent Risk | Single Score | Displays the number (count) of moderate inherent risks. |
| Moderate Residual Risk | Single Score | Displays the number (count) of moderate residual risks. |
| Residual Annual Loss Exposures | Box | Calculation of the residual Annualized Loss Expectancy (ALE) |
| Residual Risk | Bubble | Calculation of the residual risk score from the likelihood and significance of a risk. |
| Residual Risk Heatmap | Heatmap | Total number of residual risks by very high risk, high risk, moderate risk, low risk, very low risk |
| Risk by Entity | Bar | Number of total active risks broken down by profile. |
| Risk Exceptions | List | Listing of all risk exceptions |
| Risk Issues by Framework (Opened Date) | Line | Total number of open risks over time broken down by framework |
| Risks by Category | Horizontal bar | Total number of open risks broken down by category |
| Risks by Response | Horizontal bar | Total number of open risks broken down by response |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Name | Type | Description |
|---|---|---|
| Very High Inherent Risk | Single Score | Displays the number (count) of very high inherent risks. |
| Very High Residual Risk | Single Score | Displays the number (count) of very high residual risks. |
| Very Low Inherent Risk | Single Score | Displays the number (count) of very low inherent risks. |
| Very Low Residual Risk | Single Score | Displays the number of very low residual risks. |

## Advanced Governance, Risk, and Compliance Application Risk dashboard

The GRC **Application Risk and Compliance Overview Dashboard** provides the latest view of risk and compliance aspects for the business applications that are used in an enterprise.

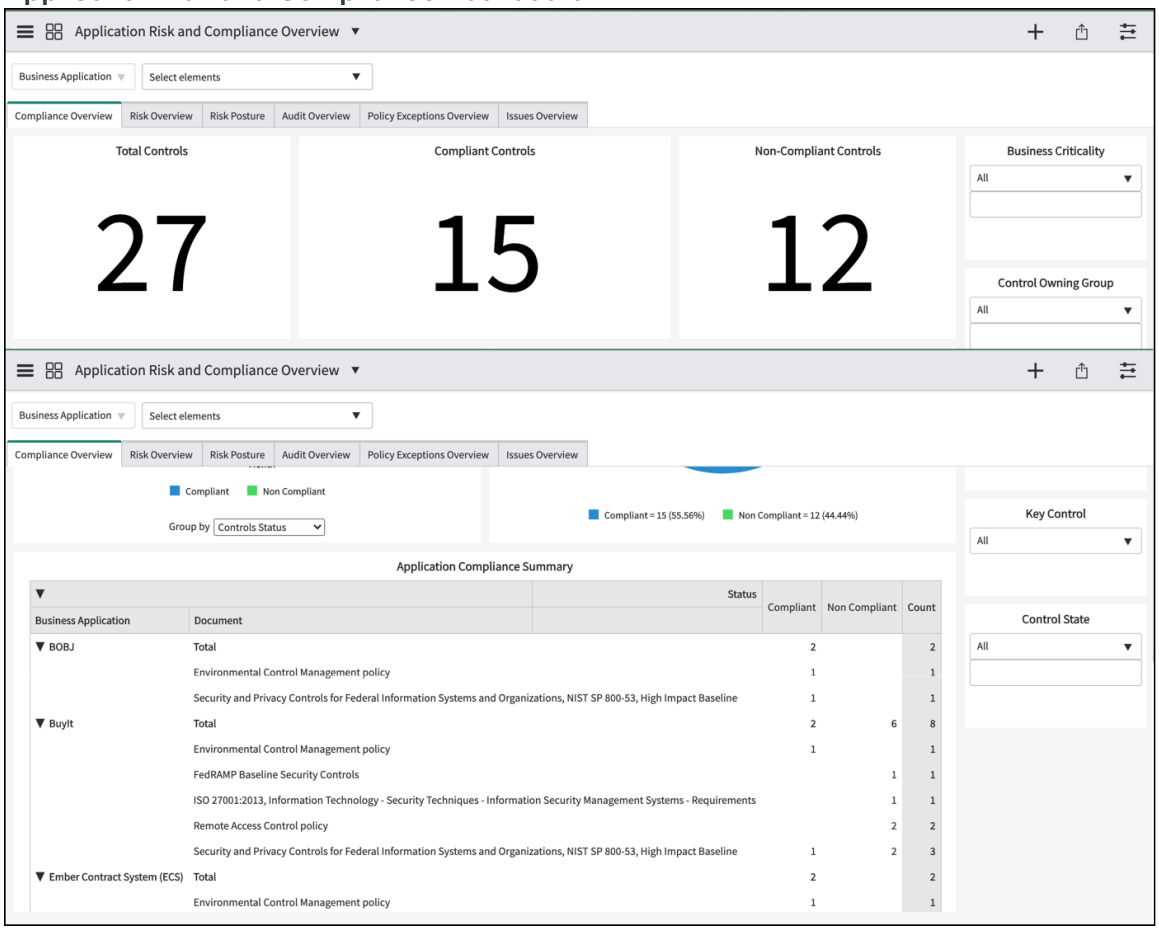
The Application Risk Dashboard is useful for the Chief Information Officer (CIO) and application owners. Both these users must have the sn_compliance.reader, sn_risk.reader, and sn_audit.user roles to view the dashboard. Navigate to **Advanced GRC Dashboard** > **Application Risk Dashboard**. The **Application Risk and Compliance Overview Dashboard** is displayed.

**Note:** To be able to view this dashboard, you must activate the GRC: Advanced Dashboards (com.sn_grc_pa_advanced) plugin and the GRC: Policy and Compliance Management (sn_compliance) plugin.

The Application Risk and Compliance Overview dashboard provides you a detailed report of the risk and compliance posture of all the business applications in an organization.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Application Risk and Compliance Dashboard




This dashboard highlights the following:

- The compliance impact of applications in use.
- The risk posture of applications.
- The state of remediation and exceptions activity of the issues.
- The audit activity around applications and status.

This dashboard provides answers to the following questions that are of interest to the CIO and the application owner:

1. What are the key applications, and are they all operational and delivering the required services optimally?
2. What are the policies and authority documents that the applications must be compliant to? Are the applications compliant to them?
3. What are the risks faced by the applications? Are any of them high to raise a concern? Are there enough mitigations in place? Are there adequate controls in place and are they working effectively?
4. For applications that need remediation, are the remediations being done on time according to the Service Level Agreements (SLAs)? Which are the applications that generate the maximum number of issues?
5. Are exceptions being sought often on the applications and why? Are they within manageable limits?
6. Are the applications due for audit any time? How have the applications performed on these audits?

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The dashboard offers various representations such as bar graphs, donut charts, and trend charts. Application owners can use various filters on the dashboard to view reports related to the business applications they own such as, critical business applications, mandated controls related to specific business application, or high priority issues and so on.

## Compliance Overview

The Compliance Overview tab appears when you activate the Policy and Compliance plugin. The Compliance Overview tab provides an overview of the compliance posture of the business applications and displays the following reports:

- Total Controls: This report provides the total number of active controls.
- Compliant Controls: This report provides the total number of compliant controls which are not in draft or retired state.
- Non-Compliant Controls: This report provides the total number of non-compliant controls which are not in draft or retired state.
- Compliance Status By Month: This report provides the number of active controls by month.

  **Note:** This bar chart shows the compliance status for the current month and can be grouped by either Control Status or Business Application.

- Compliance %: This report provides the percentage of different statuses of active controls such as Compliant, Non Compliant, and Not Applicable.
- Application Compliance Summary: This report provides the summary of policies, authority documents, and the controls associated with business applications.

The following filters can be used to filter data on the reports:

- Business Application
- Business Criticality
- Entity Owner
- Enforcement such as mandatory or voluntary controls
- Key Control
- Control State
- Control Owning Group

## Risk Overview

The Risk Overview tab appears when you activate the Advanced Risk plugin. The Risk Overview tab provides an overview of the risks associated with business applications and displays the following reports:

- Risk Heatmap by Application Criticality: This report displays the heatmap of the application risks based on criticality of applications versus the risk rating of the application.
- Risk Response Tasks Overview: This report displays the response tasks created for a risk and different states of those tasks.

  **Note:** This bar chart can be grouped by and stacked by risk response, risk response state, risk calculated score, risk response assigned to, or business application.

- Application Risk Summary: This report displays the summary of risks directly associated with the applications that contribute to the overall risk rating of the application. Other

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

downstream risks that contribute to the application risk rating are not represented in this report. The risks considered for this report are very high, high, and moderate.

- Application Risk Mitigating Controls Status: This report provides the information for an application's risks and the associated controls. The risks considered for this report are very high, high, and moderate. The state of controls must not be in draft or retired. The risks for only one year are displayed.

The following filters can be used to filter data on the reports:

- Business Application
- Criticality
- Risk Rating
- Application Owner
- Business Owner

## Risk Posture

The Risk Posture tab appears when you activate the Risk plugin. The Risk Posture tab provides information about the risk exposure of business applications. The reports in this tab can also be filtered using the Business Application filter. The Risk Posture tab displays the following:

- Very High Risks: This report displays the very high risks of an application.
- High Risks: This report displays the high risks of an application.
- Moderate Risks: This report displays the moderate risks of an application.
- Acceptance Task Expirations: This report displays the risk response acceptance tasks that have an expiration on the current day, the current week, the current month, the current quarter, and the current year.
- Contributing Risks Trend: This report displays the trend of risks directly associated with business applications and how they are performing over a period. Other downstream risks that contribute to the application risk rating are not represented in this report.

## Audit Overview

The Audit Overview tab appears when you activate the Audit plugin. The Audit Overview tab provides an overview of audit and audit activities related to business applications and displays the following reports:

- Open Audit Engagements: This report displays the number of audit engagements in open state.
- Ineffective Controls: This report displays the number of ineffective controls for an audit engagement.
- Open Issues: This report displays the number of open issues for an audit engagement.
- Past Due Issues: This report displays the number of past due audit issues for an application.
- Upcoming Audit Engagements: This report displays the monthly count for the upcoming audit engagements.
- Open Issues by Audit Engagements: This report displays the monthly count for the open audit issues.
- Past Due Issues by Audit Engagements: This report displays the past due audit issues over a period.
- Ineffective Controls by Audit Engagements: This report displays the information regarding audit engagements and the associated ineffective controls.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following filters can be used to filter data on the reports:

- Business Application
- Audit Engagement
- Criticality

## Policy Exceptions Overview

The Policy Exceptions Overview tab appears when you activate the Policy and Compliance plugin. The Policy Exception Overview tab provides information about policy exceptions requested for business applications. The data displayed in the Policy Exceptions Overview tab can be filtered using the Business Application filter. This tab displays the following reports:

- New Exceptions: This report provides information about the new exceptions requested.
- Approved Exceptions: This report provides information about the number of approved exceptions.
- Rejected Exceptions: This report provides information about the number of rejected exceptions.
- Expired Exceptions: This report provides information about the number of expired exceptions.
- Exceptions Awaiting Approval: This report provides information about the exceptions that are awaiting approval and are due on the current date, the current week, the current month, and the current quarter.
- Extensions Awaiting Approval: This report provides information about the extensions that are awaiting approval and are due on the current date, the current week, the current month, and the current quarter
- Upcoming Exceptions Expirations: This report provides information about the exceptions that are about to expire and which are due on the current date, the day after the current date, the current week, the week after the current week, and the current month.
- Exceptions Requested vs. Approved: This report provides information about the exceptions requested versus the number of exceptions approved per month.

## Issues Overview

The Issues Overview tab appears when you activate either the Risk Management plugin or the Policy and Compliance Management plugin. The Issues Overview tab provides information about the various compliance and risk issues associated with business applications. The data displayed in the Issues Overview tab can be filtered using the Business Application filter. This tab displays the following reports:

- Open Issues: This report displays the number of issues in open state.
- Critical Priority Issues: This report displays the number of critical priority issues.
- High Priority Issues: This report displays the number of high priority issues.
- Accepted Issues: This report displays the number of issues that are accepted.
- Past Due Issues: This report displays the number of past due issues.
- Issues to be Resolved: This report displays the number of issues that must be resolved on the current date, the current week, current month, current quarter, and current year.
- Remediation Tasks to be Completed: This report displays the number of remediation tasks that must be completed on the current date, the current week, current month, current quarter, and current year.
- Past Due Issues: This report displays the number of past due issues over a time period.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Past Due Remediation Tasks: This report displays the number of past due remediation tasks over a time period.
- Issue Creation Trend: This report displays the trend of how issues are created over a time period.
- Issue Closure Trend: This report displays the trend of how issues are closed over a time period.
- Remediation Task Creation Trend: This report displays the trend of how remediation tasks are created over a period.
- Remediation Task Closure Trend: This report displays the trend of how remediation tasks are closed over a period.

## Performance Analytics dashboards for risk events and risk hierarchy

Use the Performance Analytics (PA) dashboards to view the comprehensive data for risk events and risk hierarchy. Use the Analytics Hub to view data for any time period.

By default, users with the sn_risk.manager role can view data for six months. To view the data for different time periods, purchase and activate the Performance Analytics Premium plugin. Users with the sn_risk.manager role can collate historical data for one year by running the ServiceNow® Governance, Risk, and Compliance (GRC) *Entity and risk statement historical data collection* job.

**Note:** Run the historical data collection job only once. Running this job more than once leads to inconsistent data collection and might result in a loss of previous data.

## Risk Events dashboards

The Risk Events dashboards present the following data:

- Overview: This dashboard shows the following trends:
  - Gross Loss
  - Net Loss
  - Events
  - Active Events
  - Near Miss
  - Events by Type
  - Events by State
  - Top 10 Net Loss Entities
  - Top 10 Non-Financial Impact Entities
  - Top 10 Entities with Highest No. of Losses
- Risk Event Overview by Entity dashboard: Entity owners with the sn.risk_user role can view the aggregated information for gross loss, net loss, and the number of events on a monthly basis. The dashboard also shows the average gross loss per event, average net loss per event, average recovery made per event, and average additional cost per event. Entity owners with the sn.risk_user role can also view the following risk events trends for a particular entity. Administrators with the sn.risk_admin role can edit this dashboard.
  - Gross Loss
  - Net Loss
  - Events

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

  - Active Events
  - Near Miss
  - Risk Events
  - Risk Events by Non-Financial Impact
  - Annual Loss Expectancy vs Net Loss
  - Risk Event Metrics
- Overview by Risk Class dashboard: Users with the sn_risk.manager role can view level 1 risk event trends. Users can understand the aggregated gross losses, net loss, number of events created, number of active events, and the total number of near-miss events. This dashboard also shows the following trends:
  - Gross Loss
  - Net Loss
  - Events
  - Active Events
  - Near Miss
  - Top 10 Net Loss Risk Events
  - Annual Loss expectancy vs Net Loss

## Exposure by Risk Statements dashboard

To view the Exposure by Risk Statements dashboard, navigate to **Risk** > **Exposure by Risk Statements**. This dashboard is useful for users with the sn_risk.manager role. This dashboard is similar to the Exposure by Entity dashboard, except that the dashboard also displays the risks by risk statement. This dashboard provides the distribution of entities based on tolerance status and calculated scores, as well as annual loss expectancy trends. A heatmap of the risk ratings by tolerance status is included. The Exposure by Risk Statements dashboard displays the following trends:

- Risk Statements per Tolerance Status
- Risk Statements per Rating
- Annual Loss Expectancy
- Risk Ratings by Tolerance Status

## Exposure by Entity dashboard

To view the Exposure by Risk Statements dashboard, navigate to **Risk** > **Exposure by Entity**. This dashboard is useful for entity owners responsible for a particular entity class. The dashboard also shows the entity health by displaying the statuses: Unacceptable, needs attention, and acceptable. Use this dashboard to compare trends across quarters based on annual loss expectancy (ALE). This dashboard displays risk ratings by tolerance status in the form of a heatmap. The heatmap helps you identify the entities that need attention. Annual loss expectancy trends and a heatmap of the risk ratings by tolerance status are also shown. The Exposure by Risk Statements dashboard displays the following trends:

- Entities per Tolerance Status
- Entities per Rating
- Entity Annual Loss Expectancy
- Risk Ratings by Tolerance Status

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Advanced risk assessment dashboard

Use the Advanced Risk Assessment Overview dashboard for an overview of the performance of any risk assessment methodology based on the risk assessment instances.

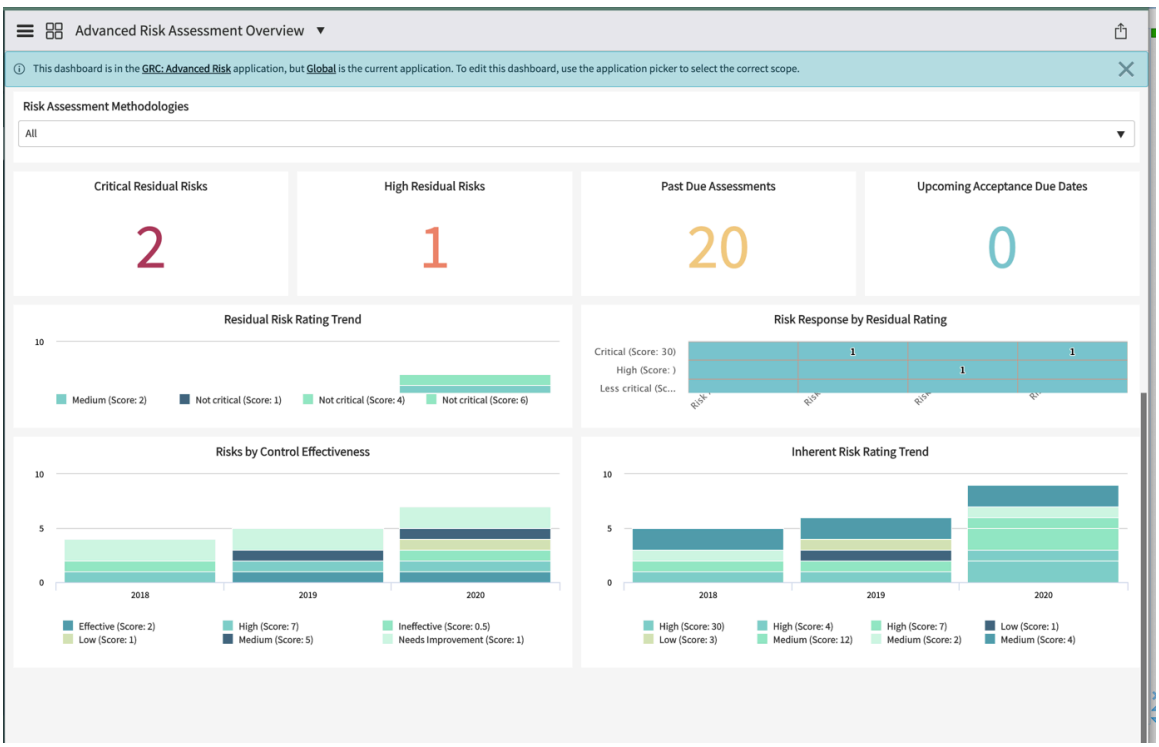
## Advanced Risk Assessment Overview

Navigate to **Advanced Risk Assessment** > **Overview**. The Advanced Risk Assessment Overview dashboard displays the following:

- Critical Residual Risks:
- High Residual Risks
- Past Due Assessments
- Upcoming Acceptance Due Dates
- Residual Risk Rating Trend
- Risk Response by Residual Rating
- Risks by Control Effectiveness
- Inherent Risk Rating Trend
- Upcoming acceptance due dates: This number indicates the count of the tasks for which the acceptance due date is within the next 30 days.

This dashboard is visible only to users with the sn_risk.manager role.

### Advanced risk dashboard



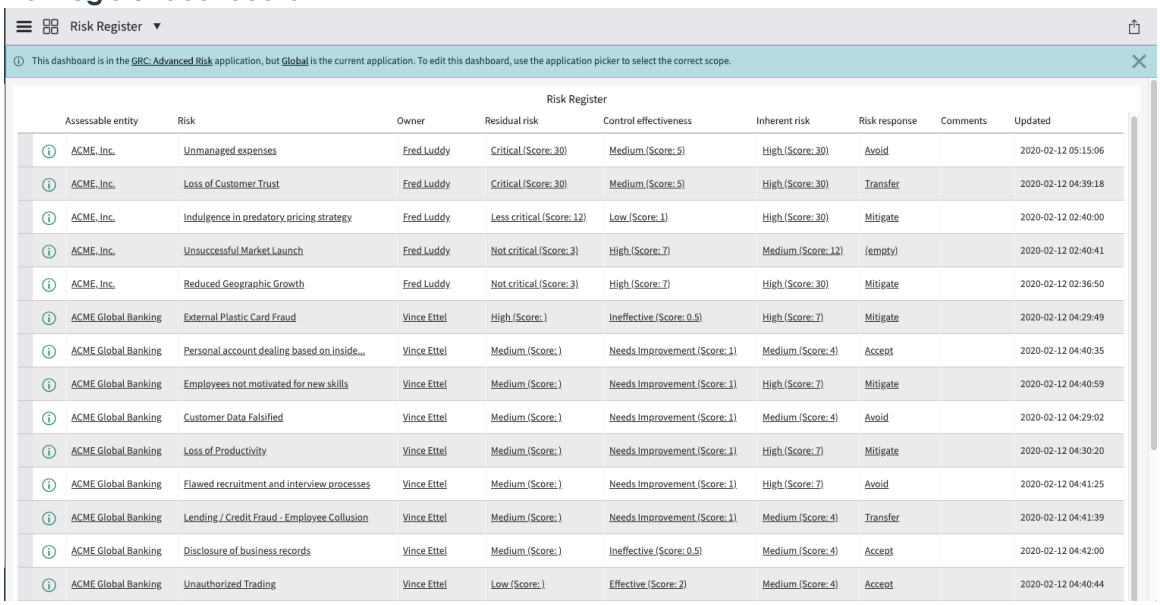

## Advanced Risk Assessment Risk Register

The Risk Register dashboard displays the risk assessments instances in the list view sorted by residual risks.

This dashboard is visible to users with the sn_risk.user role.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Risk register dashboard




Risk Register

| Assessable entity | Risk | Owner | Residual risk | Control effectiveness | Inherent risk | Risk response | Comments | Updated |
|---|---|---|---|---|---|---|---|---|
| ACME, Inc. | Unmanaged expenses | Fred Luddy | Critical (Score: 30) | Medium (Score: 5) | High (Score: 30) | Avoid | | 2020-02-12 05:15:06 |
| ACME, Inc. | Loss of Customer Trust | Fred Luddy | Critical (Score: 30) | Medium (Score: 5) | High (Score: 30) | Transfer | | 2020-02-12 04:39:18 |
| ACME, Inc. | Indulgence in predatory pricing strategy | Fred Luddy | Less critical (Score: 12) | Low (Score: 1) | High (Score: 30) | Mitigate | | 2020-02-12 02:40:00 |
| ACME, Inc. | Unsuccessful Market Launch | Fred Luddy | Not critical (Score: 3) | High (Score: 7) | Medium (Score: 12) | (empty) | | 2020-02-12 02:40:41 |
| ACME, Inc. | Reduced Geographic Growth | Fred Luddy | Not critical (Score: 3) | High (Score: 7) | High (Score: 30) | Mitigate | | 2020-02-12 02:36:50 |
| ACME Global Banking | External Plastic Card Fraud | Vince Ettel | High (Score: ) | Ineffective (Score: 0.5) | High (Score: 7) | Mitigate | | 2020-02-12 04:29:49 |
| ACME Global Banking | Personal account dealing based on inside... | Vince Ettel | Medium (Score: ) | Needs Improvement (Score: 1) | Medium (Score: 4) | Accept | | 2020-02-12 04:40:35 |
| ACME Global Banking | Employees not motivated for new skills | Vince Ettel | Medium (Score: ) | Needs Improvement (Score: 1) | High (Score: 7) | Mitigate | | 2020-02-12 04:40:59 |
| ACME Global Banking | Customer Data Falsified | Vince Ettel | Medium (Score: ) | Needs Improvement (Score: 1) | Medium (Score: 4) | Avoid | | 2020-02-12 04:29:02 |
| ACME Global Banking | Loss of Productivity | Vince Ettel | Medium (Score: ) | Needs Improvement (Score: 1) | High (Score: 7) | Mitigate | | 2020-02-12 04:30:20 |
| ACME Global Banking | Flawed recruitment and interview processes | Vince Ettel | Medium (Score: ) | Needs Improvement (Score: 1) | High (Score: 7) | Avoid | | 2020-02-12 04:41:25 |
| ACME Global Banking | Lending / Credit Fraud - Employee Collusion | Vince Ettel | Medium (Score: ) | Needs Improvement (Score: 1) | Medium (Score: 4) | Transfer | | 2020-02-12 04:41:39 |
| ACME Global Banking | Disclosure of business records | Vince Ettel | Medium (Score: ) | Ineffective (Score: 0.5) | Medium (Score: 4) | Accept | | 2020-02-12 04:42:00 |
| ACME Global Banking | Unauthorized Trading | Vince Ettel | Low (Score: ) | Effective (Score: 2) | Medium (Score: 4) | Accept | | 2020-02-12 04:40:44 |

# Risk Management reference

Reference topics provide additional information such as tables, roles, and properties that are installed with the Risk Management application.

## Components installed with Risk Management

Several types of components are installed with activation of the Risk Management plugin, including tables, user roles, and scheduled jobs.

**Note:** The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

### Roles installed with Risk Management

Roles are added with activation of GRC: Risk Management.

**Roles installed**

| Role title [name] | Description | Contains roles |
|---|---|---|
| Risk Reader<br><br>[sn_risk.reader] | In addition to the inherited permissions, the risk reader has read-only access rights to the Risk application and modules. The risk reader can do the following in the GRC scope:<br>• Act on issues assigned to him.<br>• Have read access to all Indicator templates. | • sn_grc.reader<br>• survey_reader |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| | • Can act on indicator tasks assigned to them.<br>• Have read-access to indicators.<br>• Have read-access to entities.<br><br>The risk reader can do the following in the Risk Management application:<br>• Act on the Remediation tasks assigned to them.<br>• Have read-access to risks and can be an owner to a risk.<br>• Take old risk assessment.<br>• Have read-access to risk statement and risk framework.<br>• Perform advanced risk assessment.<br>• Create risk events.<br>• Work on risk event tasks and issues.<br>• Access all risk events and risk dashboards. | |
| Risk User<br><br>[sn_risk.user] | Contains the reader and business user roles in sn_grc scope, and the reader role in the Risk Management application and business user role in the sn_grc scope. In addition to the inherited permissions, the risk user can view:<br>• entity types<br>• entities<br>• risks<br>• remediation tasks<br>• control<br>• control objectives<br>• policy exceptions | • sn_grc.user<br>• sn_compliance.reader<br>• sn_risk.reader<br>• survey_reader<br>• sn_grc.business_user<br>• sn_risk_advanced.ara_creator |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| | The risk user can also create risks. The risk user can be assigned risks and has read-only access to the Policy and Compliance Management application and modules. Risk user can do everything that the risk reader can do. The risk reader can do the following in the Risk Management application:<br>• Work on risk acceptance tasks and remediation tasks.<br>• Create risks.<br>• Access the Advanced Risk related dashboards.<br>• Have read-access to the risk identification functionality of Advanced Risk and can take assessment related to risk identification.<br>• Create assessment scope. | |
| Risk Manager<br>[sn_risk.manager] | Contains the reader, user, and manager roles in sn_grc scope, and the reader and user roles in the Risk Management application. In addition to the inherited permissions, the risk manager can do the following in the GRC scope<br>• Create issues and issue ratings.<br>• Create entity, entity types, and entity classes and class rules.<br>• Create content references.<br>• Create indicators and indicator templates.<br>• Have read-access to entity tier. | • sn_grc.manager<br>• sn_risk.user |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| | In the Risk Management application, the risk manager can:<br>• Create risk frameworks<br>• Create risk statements<br>• Create risks<br>• Create risk event response template.<br>• Create risk identifications and can view the dashboard related to risk identification.<br>• Create remediation tasks.<br>• Create assessment scheduler.<br>• Associate risk statements to Information objects using Associate risk statements module. | |
| Risk Admin<br>[sn_risk.admin] | Contains the reader, user, manager, and admin roles in sn_grc scopes, and the reader, user, and manager roles in the Risk Management application. In addition to the inherited permissions, in the GRC scope, the risk admin can create an entity tier. In the Risk Management application, the risk administrator can:<br>• Delete risk frameworks.<br>• Delete entity, tables, indicator, risks, issues, tasks.<br>• Create risk statements and risks.<br>• Modify admin properties.<br>• Modify risk criteria.<br>• Create causes and consequences of risk event.<br>• Access to risk, advanced risk related properties. | • sn_grc.admin<br>• sn_risk.user<br>• sn_risk.manager<br>• sn_grc_appr.admin |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| | • Create risk identification configuration.<br>• Create a risk assessment methodology, all types of factors.<br>• Perform administrative activities. | |
| Assessment Creator<br>[sn_risk.asmt_creator] | The assessment creator is used for creating GRC risk assessment metric types. | assessment_admin |
| GRC Business User<br>[sn_grc.business_user] | Users with this role can perform the following tasks:<br>• Take risk assessment.<br>• Create risk response tasks.<br>• View risk statements.<br>• View risk assessment scope.<br>• View and report risk events.<br>• Work on assigned risk event tasks.<br>• View indicator supporting data.<br>• Respond to indicator tasks.<br>• Respond to risk identification questionnaire.<br>• Respond to metrics data tasks.<br>• Report issues.<br>• Submit issue triage requests.<br>• Work on assigned remediation tasks.<br>• Work on assigned issues.<br>• If there is an integration with Project Portfolio Management:<br>◦ View the Project Risk Overview dashboard<br>◦ Create risks from library. | None |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| | ◦ Elevate enterprise risks.<br>◦ Initiate any object assessment. | |

### Roles installed with the GRC Risk Workspace

The GRC: Risk Workspace application installs the roles for Operational risk manager and IT risk manager for the users to perform their respective tasks.

**Roles and their descriptions**

| Role title [name] | Description | Contains roles |
|---|---|---|
| Operational risk manager<br>(sn_risk_workspace.operational_risk_manager) | Operational Risk Managers are a part of the operational risk team that manages the risk posture of the organization. They can do the following tasks:<br>• Perform risk assessments<br>• View risk events related data<br>• View the heatmaps for the risk assessments<br>**Note:** The Operational risk manager role is available only when both the Risk Workspace and Advanced Risk applications are installed. | • sn_risk.manager<br>• sn_compliance.manager<br>• sn_audit.manager |
| IT Risk manager<br>(sn_risk_workspace.IT_risk_manager) | IT risk managers work with various stakeholders to ensure that IT risks are managed within the risk appetite of the organization. They can do the following tasks:<br>• Identify risks to assess<br>• Manage risk responses<br>• Create key risk indicators | • sn_risk.manager<br>• sn_compliance.manager<br>• sn_audit.manager |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Roles and their descriptions (continued)

| Role title [name] | Description | Contains roles |
|---|---|---|
| Business operational risk manager<br><br>(sn_risk_workspace.business_op_risk_manager) | Business operational risk managers are the first lines of defense for each individual line of business. They are responsible to manage the risk posture of their specific business units. | • sn_risk.user<br>• sn_compliance.user<br>• sn_audit.user |

## Properties installed with Risk Management

Properties are added with activation of GRC: Risk Management.

### Properties installed

| Name | Description |
|---|---|
| States for which the risk is active (the first state is the default active state)<br><br>sn_risk.active_states | • **Type**: string<br>• **Default value**: draft, assess, review, monitor<br>• **Location**: **Risk** > **Administration** > **Properties** |
| States for which risk is inactive (the first state is the default inactive state)<br><br>sn_risk.closed_states | • **Type**: string<br>• **Default value**: retired<br>• **Location**: **Risk** > **Administration** > **Properties** |
| Name of the assessment metric type that is used for risk assessment<br><br>sn_risk.default_assessment | • **Type**: string<br>• **Default value**: Risk Assessment<br>• **Location**: **Risk** > **Administration** > **Properties** |
| Use qualitative impact scores as input<br><br>sn_risk.qualitative_impact | • **Type**: true or false<br>• **Default value**: false<br><br>**Note:** If upgrading from Geneva (or earlier) or Helsinki (or later) and the value was previously set to true, this value is set to true after upgrading.<br><br>• **Location**: **Risk** > **Administration** > **Properties** |
| Use qualitative likelihood scores as input<br><br>sn_risk.qualitative_likelihood | • **Type**: true or false<br>• **Default value**: false<br>• **Location**: **Risk** > **Administration** > **Properties** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Properties installed (continued)**

| Name | Description |
|---|---|
| Make risk statement mandatory in risk<br><br>sn_risk.risk_statement_mandatory | • **Type**: true or false<br>• **Default value**: false.<br><br>**Note:** If false, allows risk creation with out any associated risk statement, if true risk statement is mandatory for risk creation |
| Compare risk tolerance based on<br><br>sn_risk_advanced.risk_tolerance | • **Type**: choice list<br>• **Default value**: Sum<br>• **Location**: **Risk** > **Administration** > **Properties**<br><br>**Note:** This property is only available if you activate the Advanced Risk plugin. |
| Compare calculated risk score with<br><br>sn_risk_advanced.risk_rating_config | • **Type**: choice list<br>• **Default value**: Average calculated ALE<br>• **Location**: **Risk** > **Administration** > **Properties**<br><br>**Note:** This property is only available if you activate the Advanced Risk plugin. |
| Hide upstream and downstream risks<br><br>sn_risk.hide_upstream_downstream_risks | • **Type**: true or false<br>• **Default value**: true.<br>• **Location**: **Risk** > **Administration** > **Properties**<br><br>**Note:** This property is only available if you activate the Advanced Risk plugin. |
| Auto close issue created by indicator<br><br>sn_grc.auto_indicator_issue_closure | • **Type**: yes or no<br>• **Default value**: no.<br>• **Location**: **Risk** > **Administration** > **Properties** |
| A list of tables that are available in the 'Applies to' field on the Risk form.<br><br>sn_risk.risk_applies_to_tables | • **Type**: string<br>• **Default value**: Risk Assessment<br>• **Location**: **Risk** > **Administration** > **Properties** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Tables installed with Risk Management

Tables are added with activation of GRC: Risk Management.

#### Tables installed

| Table | Description |
|---|---|
| Risk<br>[sn_risk_risk] | Extends Item table [sn_grc_item] and stores specific risks associated with entities |
| Risk Statement<br>[sn_risk_definition] | Extends Content table [sn_grc_content] and stores definitions of risks. |
| Risk Framework<br>[sn_risk_framework] | Extends Document table [sn_grc_document] and stores all risk frameworks, a collection of risk statements |
| Risk Framework to Entity Type<br>[sn_risk_m2m_framework_profile_type] | Extends Document to Entity Type table [sn_grc_m2m_document_profile_type] and is a many-to-many relationship table that is used to manage the relationships between risk frameworks and entity types |
| Entity Type to Risk Statement<br>[sn_risk_m2m_risk_definition_profile_type] | Extends Content to Entity Type table [sn_grc_m2m_content_profile_type] and is a many-to-many relationship table that is used to manage the relationships between entity types and risk statements |
| Risk Tasks<br>[sn_risk_m2m_risk_task] | Stores many-to-many relationships between risks and tasks |
| Risk Transfer<br>[sn_risk_transfer_task] | When a risk is analyzed, there are four ways to respond to it. This table provides a way for a risk manager to transfer a risk. |
| Color Setting<br>[sn_risk_color_setting] | This table is used for the reports to relate impact/likelihood with palette colors. |
| Risk Avoidance<br>[sn_risk_avoidance_task] | When a risk is analyzed, there are four ways to respond to it. This table provides a way for a risk manager to avoid a risk. For example, by having a building in California, you are exposed to earthquake risk. You can avoid this risk by choosing not to have buildings in California. |
| Risk Acceptance<br>[sn_risk_acceptance_task] | When a risk is analyzed, there are four ways to respond to it. This table provides a way with an approval process that allows a risk manager to approve (accept) or reject the risk. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tables installed (continued)**

| Table | Description |
|---|---|
| Risk Mitigation<br><br>[sn_risk_mitigation_task] | When a risk is analyzed, there are four ways to respond to it. This table provides a way for a risk manager to mitigate a risk. |
| Risk to Control<br><br>sn_risk_m2m_risk_control | Contains relationships of risks to controls. |
| Risk Statement to Control Objective<br><br>sn_risk_m2m_risk_definition_policy_statement | Contains relationships of Risk statements to Control objectives. On addition of entry to this, related risks to controls relationships get created in Risk to Control table with matching entity. |
| Risk Mitigation to Control<br><br>sn_risk_m2m_risk_mitigation_control | Controls added to Risk mitigation task as part of the task's flow to mitigate risk are added to this table. |
| Risk Relationship<br><br>sn_risk_m2m_risk_risk | Contains upstream-downstream/parent-child relationship between two risks. |
| Risk Response Task<br><br>sn_risk_response_task | Base table to Risk Acceptance, Risk Avoidance, Risk Mitigation, Risk Transfer tasks. |

**Note:** All additional tables installed by the dependent plugins are also needed for GRC: Risk Management.

## Components installed with Advanced Risk

Activating the GRC: Advanced Risk (sn_risk_advanced) plugin adds or modifies several tables, user roles, and other components. The Advanced Risk plugin enables you to perform advanced risk assessments and manage risk events.

**Note:** The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

**Note:** Demo data is available for this feature.

### Tables installed with Advanced Risk

Tables are added with activation of GRC: Advanced Risk.

| Table | Description |
|---|---|
| Risk Event Task<br><br>[sn_risk_advanced_mitigation] | Track the mitigation tasks associated with the risk event reported. |
| Aggregated Risk Report<br><br>[sn_risk_advanced_risk_report_definition] | Create this definition where the customer can choose entities and associate some |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Table | Description |
|---|---|
| | risk statements with these entities to report aggregated risk scores. |
| Risk Report<br><br>[sn_risk_advanced_risk_report] | Based on the aggregated risk report definition, a record for each combination of entity and risk statement is created. The tolerance status and calculated score is also displayed. |
| Event Entry<br><br>[sn_risk_advanced_event_impact] | Impact entries for the risk event to be added by the Risk Manager during the Analyze state. |
| Risk Event to Risk<br><br>[sn_risk_advanced_m2m_event_risk] | Each risk event can be associated to applicable risks. This table enables tracking the risk event to risk relationships. |
| Risk Event<br><br>[sn_risk_advanced_event] | Tracks the loss or gain events reported by different users. |
| Associated Risk Events<br><br>[sn_risk_advanced_m2m_event_event] | A risk event can be linked to multiple other risk events. This table contains those associations. |
| Risk Event to Entity<br><br>[sn_risk_advanced_m2m_event_profile] | A Risk Manager can relate multiple entities that are impacted by the risk event. This table tracks the impacted entities linked to the risk event. |
| Risk Event to Control<br><br>[sn_risk_advanced_m2m_event_control] | A Risk Manager can relate multiple controls related to the entities that are linked to the risk event. This table tracks the impacted entities linked to the risk event. |
| Risk Event to Citation<br><br>[sn_risk_advanced_m2m_event_citation] | A risk manager can relate risk events to regulatory obligations and citations. This association facilitates breach reporting and compliance with regulations. |

**Note:** All additional tables installed by the dependent plugins are also needed for GRC: Advanced Risk.

### Roles for performing advanced risk assessment

When you integrate advanced risk assessment with other applications, you must ensure the users have the necessary roles to perform and approve the assessments.

Starting with version 14.1.2, several new roles have been introduced to enable users of other applications to successfully use the advanced risk assessments feature. These independent roles have been created to provide the users the required ability to perform advanced risk assessment without requiring the Integrated Risk Management specific roles such as Risk Admin, GRC Business User.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** You must manually assign the advanced risk assessment roles to the sn_grc.business_user role. To understand how you can adjust granting of roles and groups, see the How to adjust granting of roles and groups to use background jobs [KB0963693] article in the Now Support Knowledge Base. To understand more about the GRC business user role, see the GRC Business User [KB0864247] article in the Now Support Knowledge Base article in the Now Support Knowledge Base. You must log in to Now Support to view the article.

### Roles installed

| Role title [name] | Contained under | Description | Contains roles |
|---|---|---|---|
| sn_risk_advanced.ara_admin | sn_risk.admin | Users with this role can:<br>• Create risk assessment methodologies<br>• Create and manage factors | • sn_risk_advanced.ara_creator<br>• sn_risk_advanced.ara_assessor<br>• sn_risk_advanced.ara_approver<br>• sn_risk_advanced.ara_reader |
| sn_risk_advanced.ara_creator | sn_risk.user | Users with this role can create object assessments. | sn_risk_advanced.ara_reader |
| sn_risk_advanced.ara_assessor | sn_grc.business.user | Users with role can:<br>• Take assessments<br>• Perform assessment related actions such as taking the assessment and responding to or reassigning the assessment | sn_risk_advanced.ara_reader |
| sn_risk_advanced.ara_approver | sn_grc.business.user | Users with role can perform assessment related actions such as approving the assessment. | sn_risk_advanced.ara_reader |
| sn_risk_advanced.ara_reader | sn_risk.reader | Users with role can read all the information on a risk assessment instance. Users with this role have read access to all tables within advanced risk assessment. If there are users who only need to have access to reports, | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed (continued)**

| Role title [name] | Contained under | Description | Contains roles |
|---|---|---|---|
| | | they can use this role. | |
| sn_risk_advanced.qualitative_risk_appetite_reader | sn_risk.user<br><br>sn_risk.reader | Users can view the qualitative risk appetite fields. | |
| sn_risk_advanced.quantitative_risk_appetite_reader | sn_risk.user | Users can view the quantitative risk appetite fields. | |

### Properties installed with Advanced Risk

Properties are added with activation of GRC: Advanced Risk. There are also properties that are available for the various capabilities such as risk events and advanced risk assessments.

## Properties for Advanced Risk

All the properties for Advanced Risk, are listed on the System Properties page. To access the System Properties page, in the filter navigator, type *sys_properties.list*.

**Advanced risk plugin properties**

| Property | Description |
|---|---|
| Maximum number of levels for risk hierarchy<br>sn_risk_advanced.risk_hierarchy_max_levels | Set the maximum number of levels of risk hierarchy.<br>• **Type**: Integer<br>• **Default value**: 5 |
| Configure risk rating<br><br>sn_risk_advanced.risk_rating_config | Compare calculated risk score with either of choices Maximum calculated ALE, Minimum calculated ALE, Average calculated ALE.<br>• **Type**: choice list<br>• **Default value**: avg<br><br>**Note:** This property works with classic risk scoring. |
| Compare risk tolerance<br><br>sn_risk_advanced.risk_tolerance | Compare risk tolerance based on either of the choice Average, Maximum, Minimum, Sum.<br>• **Type**: choice list<br>• **Default value**: sum |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Advanced risk plugin properties (continued)**

| Property | Description |
|---|---|
| Enable the GRC enterprise risk licensing features sn_risk_advanced.enable_irm_advanced_risk_enterprise | This property enables the GRC enterprise risk licensing features.<br>• **Type**: true or false<br>• **Default value**: false |

## Properties for Risk Events

To access the risk event properties, navigate to **All** > **Risk Events** > **Administration** > **Properties**.

**Risk event properties**

| Property | Description |
|---|---|
| Show Basel attributes and reports sn_risk_advanced.show_basel_attr_reports | Set this property to true if you want to enable the Basel categorization of risk events. This property is useful for customers in the banking domain.<br>• **Type**: True or false<br>• **Default value**: false |
| Make risk event to risk relationship mandatory sn_risk_advanced.make_riskevent_to_risk_relation_mandatory | Set this property to true if you want to ensure that each risk event has corresponding risks.<br>• **Type**: True or false<br>• **Default value**: false |
| No. of days for Rapid Recovery Classification sn_risk_advanced.no_of_days_for_rapid_recovery_classification | Customize the number of days that users can set as their rapid recovery threshold.<br>• **Type**: Integer<br>• **Default value**: 5 |
| Show ORX External events sn_risk_advanced.show_orx_events | Users can choose to see the ORX External Events. ORX provides a platform for the secure exchange of high-quality operational risk loss data from around the world. This property is useful for customers in the banking domain. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Risk event properties (continued)**

| Property | Description |
|---|---|
| | Customers import the ORX information as shared by the ORX organization. This information can be related to risk statement or control objectives. This information can be modified by users.<br>• **Type**: True or false<br>• **Default value**: false |
| How many years of risk event data to be shown on the report.<br>sn_risk_advanced.number_of_years_report_data | Select how many years of risk event data must be shown on the report.<br>• **Type**: Integer<br>• **Default value**: 2<br>**Note:** This property is visible on the System Properties page. |

## Properties for advanced risk assessment

To access the advanced risk assessment properties, navigate to **All** > **Advanced Risk Assessments** > **Administration** > **Properties**.

**Properties for Advanced Risk Assessment**

| Property | Description |
|---|---|
| Migrate to Advanced Risk Assessments<br>sn_risk_advanced.hide_risk_legacy_lifecycle | Migrate to Advanced Risk Assessments.<br>• **Type**: yes or no<br>• **Default value**: no |
| Enable Advanced Risk PPM Integration<br>sn_risk_advanced.enable_advanced_risk_ppm_integration | Perform project risk assessments. Only users with the it_pps_admin or sn_risk.admin roles can enable this property.<br>• **Type**: yes or no<br>• **Default value**: no |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Properties for Advanced Risk Assessment (continued)**

| Property | Description |
|---|---|
| | For more information, see Configure Project Portfolio Management and Advanced Risk integration<br><br>**Note:** This property is only available when Project Portfolio Management is installed. |

## Business process roles

Various roles are available for business process users and managers.

The following table lists the roles that you must use for managing your business processes.

**Roles used for managing business processes**

| Role title | Description |
|---|---|
| Business process administrator<br><br>business_process_admin | This role provides create, read, update, and delete (CRUD) access to all records and their relationships in the business process. This role is assigned to users who are administrators and have thorough information and training on business processes. In the context of GRC, users with the sn_grc.admin role who manage GRC applications and their setup automatically gain access to this role. This access enables the GRC administrators to administer business process and its records similar to other GRC tables. |
| Business process manager<br><br>business_process_manager | This role is assigned to business process managers who are usually specialists and manage multiple business processes in the organisation. They can create, read and update any business process and manage the relationship of business process with other records. Such users generally work with other employees and are experts around business processes. In the context of GRC, users with the sn_grc.manager role automatically inherit this role that enables them to manage the business processes for the entire organization. |
| Business process user<br><br>business_process_user | This role must be assigned to the respective process owners who manage the business process that they own. With this role, they can update the business processes that they own and can also read any business |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles used for managing business processes (continued)**

| Role title | Description |
|---|---|
| | process. This role can also be provided to users who are required to view the business processes in the organization and understand them better. In the context of GRC, users with the sn_risk.user role are automatically assigned this role as this role enables them to manage the business processes they own as well as read all business processes. |

# Third-party Risk Management

The ServiceNow® GRC: Third-party Risk Management (TPRM) application enables you to proactively identify, assess, and mitigate risks that are associated with your third-party relationships. TPRM provides a centralized process for managing your portfolio of third parties, assessing and scoring risk, and performing remediation.

## Get started

Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release note information for all released apps, see the ServiceNow Store version history release notes.

### Explore



Learn about how third-party risk managers, third-party risk users, and third-party risk administrators use the Third-party Risk Management application.

### Configure



You can activate or upgrade TPRM, by downloading the applications from the ServiceNow Store and then configuring the settings to meet your needs.

### Request third-party risk due diligence



Request third-party risk due diligence to determine the level of risk for interactions with a third party and their engagement.

### Assess third-party risk



Use Third-party Risk Management to identify and assess

### Monitor third-party risk



Use the Third-party Risk Management application to monitor potential risks

### Approve or reject requests for due diligence



Use the Third-party Risk Management

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

potential risks that are associated with your third-party relationships.

associated with your third-party relationships.

application to approve or reject new requests for due diligence, after reviewing questionnaire responses and due diligence process results.

Manage the contract risk process



Protect your organization's interests, as the Third Party Risk contract negotiator by incorporating specific contractual provisions so that you can address identified risks.

Work in the VRM classic user interface



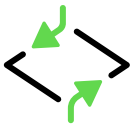
Use the legacy user interface to perform all Vendor Risk Management tasks.

Integrate scores from risk intelligence providers



Integrate scores from risk intelligence providers. The scores provide insight on how trustworthy and safe a particular third party can be.

Use the third-party portal



Use the third-party portal to respond to questionnaires, requests for documentation, tasks, and issues. The portal is the point of interaction between third-party contacts and risk assessors.

Reference



Reference topics provide detailed descriptions of tables, properties, forms, and roles that are installed with the Third-party Risk Management application.

### Troubleshoot and get help

- Ask or answer questions in the GRC community.
- Search the Known Error Portal for known error articles.
- Learn how to build apps on the developer site.
- Contact Customer Service and Support.

## Exploring Third-party Risk Management

The Third-party Risk Management application centralizes and standardizes the processes, source materials, responsible persons, and methods of your third-party risk management

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

program. You can improve your operations by managing your portfolio of third parties and by identifying, tracking, and mitigating the issues that arise with third parties.

## Third-party Risk Management overview

To protect your organization's assets, reputation, and operations, your third-party risk management program must identify, assess, and mitigate the risks that are associated with external parties. The TPRM application helps you to prevent your outsourced providers, partners, and suppliers from creating a business disruption or a negative impact on your business performance. By using the TPRM application, you can reduce the manual burden and costs of your risk assessment process through automation.

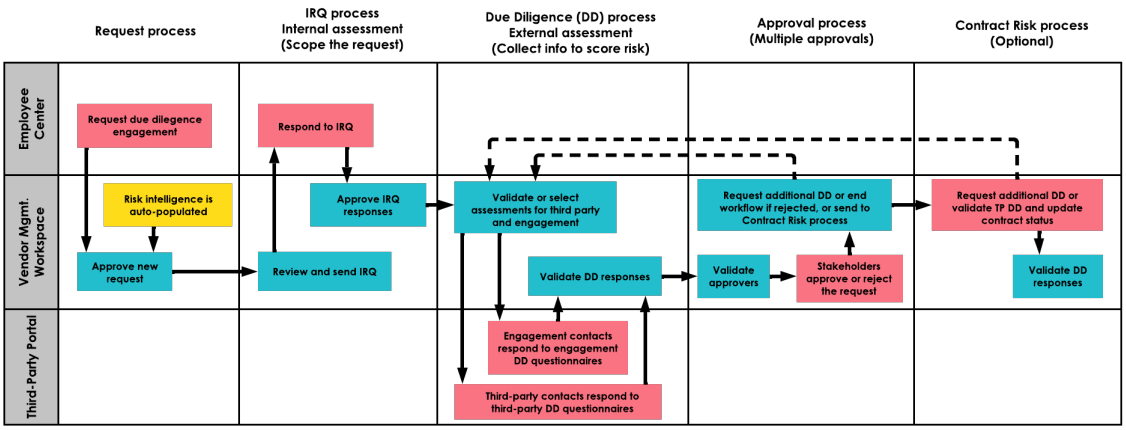
TPRM brings all third-party risk information into one environment.

The following key capabilities can help you to assess risk more effectively:

- Onboarding, Offboarding, Renewals, and additional due diligence workflows
- Assessment management
- Continuous risk monitoring
- Risk performance management

## Third-party Risk Management workflow

The following infographic shows the workflow of the most important processes that you can use to manage risk.




## High-level workflow steps

1. An internal employee requests due diligence on a new third party or engagement. See Terminology for more information.
2. After they make the request, the Third-party risk (TPR) manager approves the request for an Inherent Risk Questionnaire (IRQ). The IRQ is a set of questions that scores and scopes the required due diligence on the third parties or engagements.
3. After the assigned assessor completes the IRQ, the TPR manager reviews and approves it.
4. Any external third-party questionnaires that are selected by the TPR manager are automatically sent out. If you have any integrated risk intelligence, relevant information is pulled at this time.
5. The information is scored and combined into one single view of the due diligence process to display all scores, completed questionnaires, issues, approvals, and comments.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. All approvers can review due diligence and see the detailed information before they make an approval.
7. After all approvers approve the due diligence request, all the due diligence information can be made available for the person that is negotiating the contract. The contract risk process only applies if a contract is required.
8. The contract negotiator can see the detailed information of all the scores and questionnaires. If additional due diligence is required, they can request it.
9. If the contract negotiator successfully executes a contract with the third party, they can upload it and specify that the contract is executed. This action automatically notifies all key stakeholders of the contract's status.
10. The contract negotiator can also specify that the contract isn't executed and that the third party isn't engaged for business.

For an in-depth description of the TPRM Due diligence workflow, see Due diligence workflow.

## Third-party Risk Management benefits

The following table shows the benefits of the Third-party Risk Management application.

| Benefit | Feature | Users |
|---|---|---|
| View important risk information and quickly access actions. | TPRM Home page | All TPRM users |
| Use due diligence management reports to track, prioritize, and manage responsibilities. | TPRM Due diligence management reports | All TPRM users |
| Identify and assess the potential risk that is associated with your third-party relationship. | TPRM Risk activity page | All TPRM users |
| Pinpoint the geographical locations of active third parties and engagements. You can configure filters to view particular risk ratings and engagement types. | TPRM Risk concentration map | All TPRM users |
| Prioritize assessments, issues, and tasks that need attention. | TPRM Risk activity page | All TPRM users |
| Access tasks that are assigned to you and to members of your group. | TPRM Task page | All TPRM users |
| Access all items that you can view or act on in TPRM. | TPRM List page | All TPRM users |
| Use the engagement page to access all current information and status for a third party or engagement. | Get an overview of a third party or engagement | All internal users |
| Import existing data (third parties, engagements, assessments, questionnaires, issues, and so on) from other systems (like the Aravo platform, the ProcessUnity platform, and so on). You aren't charged for importing the data. | Import existing data from other systems | TPR Managers and TPR Admins |
| Work on all processes in the workflow for a due diligence request: IRQs, external | Monitoring the due diligence request process | TPR Managers and TPR Admins |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Benefit | Feature | Users |
| --- | --- | --- |
| due diligence, approval, contract risk, and closed requests. | | |
| Use the third-party portal as a primary point of interaction for third parties and risk assessors. | Managing the Third-party portal | TPR Managers, TPR Assessors, and Third parties |

## Risk profile

A risk profile is a comprehensive assessment of the potential risks that are associated with a particular third party. To generate a risk profile, you evaluate and document several aspects of the third party's operations, practices, and relationships. The aim is to understand the level of risk they may pose to your organization.

A risk profile enables you to make informed decisions about engaging, monitoring, and mitigating risks associated with third parties. Identify areas of concern, implement risk mitigation strategies, and establish ongoing monitoring processes to help you align third-party relationships with your risk tolerance and strategic objectives.

To prioritize and manage risks effectively, you assign scores or ratings to many risk factors and aggregate them to generate an overall risk assessment for the third party. TPRM displays risk profile information on the Home page.

## Components of a third-party risk profile

Third-party information

Basic details such as name, location, contact information, size, and ownership structure.

Composite Risk Ratings

- IRQ results
- External risk assessment ratings
- Engagement ratings
- Risk intelligence ratings

Risk domain

- Financial stability: An assessment of the third party's financial health to gauge their ability to fulfill their contractual obligations. This includes factors like revenue, profitability, and debt levels.
- Operational risk: An evaluation of the third party's business operations and processes, including their ability to deliver products or services consistently and reliably.
- Compliance and legal risk: A review of the third party's adherence to relevant laws, regulations, and industry standards. This may include assessments of their compliance with data protection, security, and ethical standards.
- Cybersecurity risk: An assessment of the third party's cybersecurity measures and data protection practices to determine their ability to safeguard sensitive information.
- Geopolitical risk: An analysis of geopolitical factors that could impact the third party's operations, such as political stability and regulatory changes in their home country.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Reputation risk: Consideration of the third party's reputation in the industry, including any past incidents or controversies that could affect the organization's brand.
- Business continuity risk: An evaluation of the third party's plans and capabilities for maintaining operations if there are disruptions or disasters.

Risk intelligence

Risk intelligence providers generate risk scores for a variety of third-party risk domains. Your organization can purchase services from providers that return data that is analogous to personal credit scores. The scores provide insight on how trustworthy and safe a particular third party can be.

## Why you conduct due diligence

Conducting due diligence on third parties is a crucial component of your comprehensive third-party risk program. You conduct due diligence to become aware of the risks that are associated with a third party so that you can confidently decide how to form your relationship.

Third-party risk management concentrates on evaluating and managing the risks introduced by external parties. This includes assessing factors such as cybersecurity risks, data privacy compliance, financial stability, regulatory compliance, and operational resilience associated with the engagements. You conduct due diligence (an investigation or examination of business relationship risk), to make informed decisions, establish appropriate controls, and mitigate the potential negative impact of engaging with third parties.

## Goals of due diligence

Comply with regulations

Companies are often subject to various regulations and legal requirements that mandate conducting due diligence on third parties. These regulations aim to prevent illegal activities, such as money laundering, corruption, fraud, and other forms of financial misconduct. By performing due diligence, you demonstrate your commitment to compliance and risk mitigation. See Regulations that affect third-party risk.

Protect your reputation

Engaging with a third party can directly impact a company's reputation. By conducting due diligence, you can uncover any potential negative associations or activities that could harm your brand image or public perception. This enables you to make informed decisions about whether to proceed with the engagement or to take appropriate mitigating actions.

Safeguard against operational disruptions

Third parties such as suppliers, service providers, or partners play critical roles in your organization's operations. Poor performance, financial instability, or other issues with third parties can disrupt your operations and supply chain, leading to delays, quality issues, or other problems. Due diligence helps assess the reliability and capability of third parties, reducing the risk of operational disruptions.

Protect sensitive information

You might share sensitive information with third parties, such as customer data, intellectual property, or trade secrets. Due diligence helps evaluate a third party's data security measures, privacy practices, and overall commitment to protecting confidential information. This is crucial for maintaining data integrity and helping to prevent breaches or unauthorized disclosures.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Mitigate financial risks

Engaging with financially unstable third parties can pose significant financial risks. Due diligence helps assess the financial health, creditworthiness, and payment history of potential partners or third parties. It enables you to evaluate the financial risks associated with a third party and to make informed decisions based on their financial stability and track record.

Comply with internal policies

You might have internal policies and standards that dictate the criteria for engaging with third parties. Due diligence helps ensure that potential third parties align with the policies, such as sustainability practices, diversity and inclusion requirements, or ethical guidelines.

Related topics

Types of due diligence

### Types of due diligence

In the due diligence process, you typically conduct several types of due diligence to gather relevant information and assess various aspects of the third party. The particular types of due diligence that you conduct vary depending on the nature and criticality of the engagement and the risks involved.

Information Security due diligence

Information security due diligence is critical. It involves evaluating the third party's data protection practices, cybersecurity measures, and information handling processes. This includes assessing their data security policies, incident response capabilities, encryption practices, and employee training on data protection. The objective is to safeguard sensitive information and mitigate the risk of data breaches or unauthorized access.

Financial due diligence

Financial due diligence involves assessing the financial health and stability of the third party. It includes reviewing financial statements, analyzing profitability, liquidity, debt levels, cash flow, and other financial indicators. The goal is to understand the financial viability of the third party and help ensure that they have the capacity to fulfill their obligations.

Legal due diligence

Legal due diligence involves examining the legal and regulatory compliance of the third party. It includes reviewing contracts, agreements, licenses, permits, and legal documents. The purpose is to identify any legal risks, liabilities, ongoing litigation, or regulatory non-compliance that could impact your organization's interests.

Operational due diligence

Operational due diligence focuses on assessing the operational capabilities and processes of the third party. It involves evaluating their infrastructure, facilities, supply chain, production processes, quality controls, and capacity to meet your organization's requirements. The goal is to help ensure that the third party can effectively deliver the desired products or services.

Compliance due diligence

Compliance due diligence involves verifying the third party's adherence to applicable laws, regulations, and industry standards. It includes assessing their compliance programs, policies, and procedures related to areas such as anti-

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

corruption, data privacy, information security, environmental practices, and labor standards. The objective is to identify any compliance gaps or risks that could result in legal or reputational issues for your organization.

Reputation due diligence

Reputation due diligence focuses on evaluating the third party's reputation, integrity, and past performance. It involves conducting background checks, reviewing references, searching for news or media coverage, and assessing any past controversies or ethical issues. The purpose is to help ensure that the third party has a positive reputation and aligns with your organization's values and expectations.

## Why you might have several engagements with a single third party

While onboarding a particular third party, you might conduct a separate engagement for each distinct type of relationship that you have with the third party. One engagement is to assess the risk involved in the third party's development of software for your organization and a separate engagement is for the facilities management service that they provide.

## Different engagements of the same third party might require varying levels of risk assessment

**Note:** The first internal step after an engagement request is approved is to start the IRQ process to scope the risk by determining the third party's risk score. An engagement starts in the inactive state. An engagement moves to the active state when a contract is in place or you take part in an active relationship with the third party.

Different engagements of the same third party can require different levels of risk assessment due to variations in the nature of the services provided, the level of access to sensitive data or critical systems, and the potential impact on your organization's infrastructure. By conducting a separate risk assessment for each engagement, you can tailor your risk management strategies and controls to address the risks associated with each engagement effectively.

## Example — the third party will provide two distinct services

In this example, Your organization engages with a third party for two distinct services:

Service: Software Development Engagement

The third party is responsible for developing a custom software application for the financial institution. This engagement involves the third party accessing and processing sensitive customer data, integrating with critical systems, and potentially introducing changes to the organization's infrastructure.

Service: Facilities Management

The third party is also responsible for managing the physical security and maintenance of the financial institution's office buildings. This engagement involves providing security personnel, managing access control systems, and confirming the overall safety and maintenance of the facilities.

The services present different risk profiles and require separate risk assessment engagements:

Engagement for the software development service

This engagement involves a higher level of risk due to the following factors:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Access to sensitive data: The third party has access to customer data, which requires strict data protection and privacy controls to help prevent unauthorized access or data breaches.
- System integration: The third party's software must integrate with critical systems, potentially impacting the stability, availability, or security of those systems. Proper testing and quality assurance procedures are crucial to minimize the risk of system failures or vulnerabilities.
- Change management: The introduction of new software or changes to existing systems can introduce risks, such as compatibility issues, system disruptions, or software vulnerabilities. Robust change management practices and code review processes are necessary to mitigate these risks.

Engagement for the facilities management service

Even though this engagement also involves the same third party, the risk profile is lower when compared to the software development engagement:

- Physical security: The focus here is on managing physical security measures, such as access control and surveillance systems. While still important, the risks associated with physical security are typically more straightforward and easier to manage compared to cybersecurity risks.
- Maintenance and safety: The third party's responsibility is primarily related to general maintenance and promoting a safe working environment. While there are still risks associated with building maintenance (for example, safety hazards), they might be more predictable and manageable compared to the complex cybersecurity risks in the software development engagement.

### Types of engagement with third parties

The particular third-party engagements that you might have depend on your industry, size, and operational requirements. Each engagement brings its own set of risks and requires appropriate risk management measures (due diligence) to protect your interests.

## Types of engagement

| Type of third party | Description | Possible types of engagement |
|---|---|---|
| Advertising Agencies | Companies that create and execute advertising campaigns on behalf of organizations. | Developing marketing strategies, creating ad campaigns, managing media placements. |
| Affiliates/Subsidiaries | Related companies or subsidiaries that are part of the organization's corporate structure. | Depends on the type of organization |
| Auditors | Independent firms that conduct financial audits and provide assurance services to verify the accuracy of financial statements. | Conducting financial audits, providing internal control assessments, offering risk management advice. |
| Business Partners | Companies or organizations that collaborate with the organization on joint | Joint marketing initiatives, co-developing products, sharing resources. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Type of third party | Description | Possible types of engagement |
|---|---|---|
| | ventures, partnerships, or strategic alliances. | |
| Business Process Outsourcers (BPOs) | Third-party providers that assume responsibility for specific business processes or functions. | Customer support, payroll processing, IT helpdesk support. |
| Call Centers | Service providers that handle customer inquiries, support, and telemarketing activities. | Customer service hotline, technical support, sales calls. |
| Clients | Entities or individuals who engage the organization's services or purchase its products. | Client Services |
| Cloud Service Providers (CSPs) | Companies that offer cloud-based infrastructure, platforms, or software solutions. | Data storage and backup, cloud computing, software-as-a-service (SaaS) solutions. |
| Collection Agencies | Third parties engaged to recover outstanding debts or delinquent payments on behalf of organizations. | Debt collection services, skip tracing, negotiation with debtors. |
| Consultants | Individuals or firms that provide expert advice, guidance, and solutions in specific areas. | Management consulting, IT consulting, process improvement, strategy development. |
| Contractors | Individuals or companies hired to perform specific tasks, services, or projects. | Construction projects, software development, marketing campaigns, event planning. |
| Counterparties | Entities or individuals with whom the organization has contractual agreements or business relationships. | Supplier contracts, partnership agreements, licensing agreements. |
| Credit Card Processors | Entities that facilitate payment processing and manage credit card transactions. | Credit card payment processing, fraud prevention, merchant services. |
| Customers | Individuals or entities that purchase goods or services from the organization. | Product sales, service subscriptions, client contracts. |
| Datacenters | Facilities that provide secure hosting, storage, and management of digital data and IT infrastructure. | Server colocation, data backup and recovery, network management. |
| Data Processors | Third parties that process or handle sensitive data on behalf of the organization | cloud storage providers. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Type of third party | Description | Possible types of engagement |
|---|---|---|
| Digital Marketing Agencies | Agencies specializing in digital marketing strategies and tactics. | Search engine optimization (SEO), social media marketing, content creation, online advertising. |
| Distributors | Third parties responsible for distributing or selling products or services on behalf of manufacturers or suppliers. | Product distribution agreements, supply chain management, sales partnerships. |
| E-commerce Platforms | Online platforms that enable businesses to sell products or services directly to customers over the internet. | Online storefront setup, payment processing integration, order fulfillment. |
| Employee Benefits Providers | Companies that offer employee benefits administration services. | Health insurance coverage, retirement plans, employee wellness programs. |
| Energy Providers | Entities that supply electricity, gas, or other forms of energy required for organizational operations. | Energy supply contracts, utility services, energy management consulting. |
| Environmental Consultants | Experts who assess and provide guidance on environmental impact, compliance, and sustainability matters. | Environmental impact assessments, regulatory compliance consulting, sustainability planning. |
| Event Management Companies | Service providers that plan, organize, and execute corporate events, conferences, trade shows, or promotional activities. | Event planning, venue coordination, logistics management. |
| Facilities Management Companies | Third parties responsible for managing and maintaining physical facilities. | Security services, cleaning and maintenance, repairs and renovations. |
| Financial Advisors | Professionals who provide advice and guidance on financial planning, investment strategies, and wealth management. | Financial planning, investment portfolio management, retirement planning. |
| Freight Forwarders | Entities that manage and coordinate the transportation of goods. | Freight logistics, customs clearance, supply chain management. |
| Franchises | Entities or individuals granted the right to operate a business under the organization's brand and business model. | Franchise agreements, brand licensing, franchise support services. |
| Government Agencies | Government bodies or entities with which the organization interacts. | Regulatory compliance, permits and licenses, government contracts. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Type of third party | Description | Possible types of engagement |
|---|---|---|
| Human Resources Outsourcers | Service providers that handle various HR functions. | Payroll processing, employee benefits administration, recruitment outsourcing. |
| Insurance Providers/Brokers | Companies or brokers that provide insurance coverage or risk management services. | Insurance policies, risk assessments, claims management. |
| Joint Venture Partners | Companies or organizations that enter into a joint venture with the organization. | Joint business development, shared marketing campaigns, co-production agreements. |
| Legal Services Providers | Law firms or legal service providers engaged to address legal matters. | Contract drafting, litigation support, regulatory compliance advice. |
| Marketing and Advertising Agencies | External agencies or consultants engaged for marketing, advertising, or public relations activities. | Marketing strategy development, ad campaign execution, brand positioning. |
| Outsourcing Providers | Third parties that handle specific business functions or processes. | IT outsourcing, finance and accounting services, manufacturing outsourcing. |
| Regulatory/Compliance Entities | Government agencies, regulatory bodies, or compliance consultants. | Compliance audits, regulatory reporting, industry certifications. |
| Resellers/Distributors | Third parties that distribute or resell the organization's products or services. | Retail partnerships, distribution agreements, reseller networks. |
| Research and Development Partners | Universities, research institutions, or specialized R&D companies. | Collaborative research projects, technology licensing, innovation partnerships. |
| Service Providers | External entities that offer various services to support the organization's operations. | IT support, facility maintenance, consulting services. |
| Software Providers | Companies that supply software solutions to support the organization's operations. | Enterprise software licensing, software maintenance and support, customized software development. |
| Subcontractors | Third parties engaged by contractors or vendors to perform specific tasks. | Subcontracted construction work, specialized service subcontracting, project-specific outsourcing. |
| Suppliers | External entities that provide goods or materials necessary for the organization's operations. | Procurement agreements, supply contracts, and third-party partnerships. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Type of third party | Description | Possible types of engagement |
|---|---|---|
| Technology Providers | Companies that supply technology solutions, software, or hardware. | IT infrastructure deployment, software integration, network setup and management. |
| Telecommunications Providers | Companies that provide communication services, such as voice, data, and internet connectivity. | Phone and internet services, virtual private networks (VPNs), network security solutions. |
| Testing and Quality Assurance Providers | Companies that offer software testing and quality assurance services. | Software testing, quality assurance assessments, user experience testing. |
| Training and Development Providers | Entities that offer training and development programs, courses, or workshops. | Employee training, leadership development, skills workshops. |
| Transportation Providers | Entities that provide transportation services for goods or people. | Freight transportation, passenger transportation, logistics coordination. |
| Travel Agencies | Companies that assist with travel arrangements, bookings, and itinerary planning. | Corporate travel management, travel booking services, group travel coordination. |
| Utility Providers | Companies that supply essential utilities, such as water, gas, or electricity. | Water supply, gas services, electricity distribution. |
| Vendors | External entities that supply goods or services required for organizational operations. | Supply chain management, procurement contracts, and third-party partnerships. |
| Warehousing and Logistics Providers | Companies that offer warehousing, storage, and logistics services. | Inventory management, order fulfillment, distribution network management. |
| Web Development and Design Agencies | Agencies specializing in web development, design, and digital experiences. | Website development, user interface design, e-commerce platform integration. |
| Wholesalers | Entities that buy goods in bulk and resell them to retailers or distributors. | Wholesale distribution agreements, supply chain management, bulk purchasing. |
| Workforce Agencies | Agencies that provide temporary or contingent workforce solutions. | Temporary staffing, contract workers, on-demand labor. |

## Regulations that affect third-party risk

When implementing your third-party risk management program, you must carefully consider the regulations. Applicable regulations vary depending on your industry, geographic location, jurisdiction, and nature of your operations.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Regulations that typically affect third-party risk management programs

You should consult legal and compliance experts to determine the specific regulatory landscape relevant to your third-party relationships. Here's a list of regulations that are typically considered when assessing third-party risk:

Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulations

These regulations aim to prevent money laundering, terrorist financing, and other illicit financial activities. They require companies to verify the identity of their third parties, assess their sources of funds, and ensure compliance with applicable AML and CTF laws.

Anti-Corruption and Bribery laws

Regulations such as the U.S. Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act impose strict requirements on companies to prevent bribery and corruption. Due diligence helps identify any potential risks related to bribery or corruption in the third party's operations and relationships.

Data Protection and Privacy regulations

With the increasing focus on data protection and privacy, regulations like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) require companies to safeguard personal data. Due diligence includes assessing a third party's data protection and privacy practices to ensure compliance with these regulations.

Sanctions and Embargoes

Governments impose sanctions and embargoes on certain countries, individuals, or entities to restrict trade and prevent support for illegal activities. Companies need to ensure that their third parties aren't subject to any sanctions or embargoes and aren't engaged in activities that violate these restrictions.

Financial Regulations

Depending on the industry, companies might need to consider financial regulations such as the Sarbanes-Oxley Act (SOX) for publicly traded companies or sector-specific regulations like the Dodd-Frank Act for financial institutions. These regulations often require companies to assess the financial stability, reporting accuracy, and internal controls of their third parties.

Labor and Employment Laws

Companies need to ensure that their third parties comply with labor and employment laws, including regulations related to minimum wage, working hours, health and safety, and equal employment opportunities. This helps mitigate risks associated with labor violations and potential reputational harm.

Environmental Regulations

Companies might need to evaluate a third party's compliance with environmental regulations, particularly if the third party engages in activities that have an environmental impact. This includes assessing their environmental practices, waste management, pollution control measures, and adherence to sustainability standards.

## Benefits of your third-party risk management program

A third-party risk management program can help you to proactively identify, assess, and mitigate the risks that are associated with your relationships with third parties. By effectively managing third-party risks, you can enhance your overall resilience, protect your interests, and create sustainable and trustworthy business relationships.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Here are some key benefits and value propositions of implementing a robust third-party risk management program:

Risk reduction and mitigation

A third-party risk management program enables you to identify and assess potential risks associated with your third-party relationships. By conducting due diligence, monitoring activities, and implementing risk mitigation strategies, you can reduce the likelihood and impact of risks such as compliance violations, financial instability, data breaches, reputation damage, operational disruptions, and legal liabilities.

Compliance and regulatory adherence

A comprehensive third-party risk management program helps you comply with applicable laws, regulations, and industry standards. By verifying the compliance of your third parties with various regulatory requirements, you can avoid legal penalties, reputational damage, and potential business disruptions resulting from non-compliance.

Enhanced reputation and brand protection

Engaging with third parties introduces risks to your reputation and brand. By proactively managing these risks through a third-party risk management program, you can safeguard their reputation, maintain stakeholder trust, and demonstrate a commitment to ethical business practices and responsible supply chain management.

Operational efficiency and continuity

Third parties such as suppliers, vendors, or service providers play critical roles in your operations. By effectively managing third-party risks, you can validate the reliability, performance, and continuity of your supply chain. This reduces the likelihood of disruptions, delays, or quality issues that can impact operational efficiency and customer satisfaction.

Cost savings and financial protection

Implementing a third-party risk management program can lead to cost savings and financial protection. By evaluating the financial stability of third parties, you can avoid engaging with financially vulnerable entities that might default on payments or fail to deliver goods or services. Additionally, by helping to prevent legal and regulatory non-compliance issues, you can avoid costly fines, penalties, legal disputes, and associated expenses.

Enhanced decision-making and informed partnerships

A well-structured third-party risk management program provides you with comprehensive information and insights about your third parties. This enables better decision making when selecting and engaging with third parties, enabling you to choose partners that align with your values, standards, and business objectives. It also helps foster stronger and more reliable relationships based on trust and shared risk awareness.

Strengthened cybersecurity and data protection

Third-party relationships can introduce significant cybersecurity and data protection risks. A third-party risk management program helps assess the cybersecurity practices and data protection measures of third parties, reducing the chances of data breaches, unauthorized access, or data leakage. This helps you protect sensitive information and maintain compliance with data protection regulations.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Example — Onboarding a third party

Acme, a large manufacturing company, is in the process of onboarding a new third party to supply critical components for their production line. To help ensure the third party's reliability and to mitigate potential risks, Acme starts a thorough third-party risk management onboarding process.

## Onboarding process example

Request process

Any employee (typically a user who wants to do business with a third party) makes the business case to start the due diligence process for a risk assessment.

A Third-party Risk (TPR) manager reviews the request for due diligence for the engagement and approves it.

Inherent Risk Questionnaire (IRQ) process

After the request is approved, the IRQ assessor completes the internal risk assessment by responding to the IRQ.

Based on the information gathered, Acme assesses the potential risks associated with the third party. They evaluate factors such as financial stability, operational capacity, adherence to quality standards, compliance with regulations, and the third party's ability to meet delivery timelines. This assessment helps Acme understand the third party's risk profile and determine the appropriate risk mitigation strategies.

Due diligence process: Compliance verification and data security and privacy assessment

When the IRQ process is complete, Acme's TPRM application sends questionnaires and requests for documentation to the third party. As part of an assessment, you might send multiple questionnaires and document requests. Acme might request documents: the third party's certifications, licenses, or audit reports to validate compliance.

**Note:** To simplify and automate the process of determining which questionnaires and document requests to send to a third party of this type, Acme's staff has developed assessment templates. They defined questionnaire templates, document request templates, or both and then grouped them into an assessment template. Acme can reuse the template to send the appropriate questionnaires, document requests, or both to similar third parties in future assessments.

Acme uses the third party's responses and internal analysis to determine whether the third party meets all necessary compliance requirements. This includes verifying the third party's compliance with applicable laws and regulations, such as environmental regulations, labor laws, and anti-corruption policies.

Given the sensitive nature of the components involved, Acme evaluates the third party's data security and privacy practices. They assess the third party's information security measures, data protection policies, access controls, and vulnerability management processes. If the third party will have access to Acme's proprietary information or customer data, they might require the third party to undergo a cybersecurity audit or provide evidence of their data protection measures.

Contractual Agreements and Risk Mitigation

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

To protect their interests, the TPR contract negotiator at Acme (often corporate counsel) incorporates specific contractual provisions to address identified risks. The contract negotiator uses the information gained in the IRQ and due diligence processes to include clauses related to compliance, quality standards, confidentiality, data protection, business continuity, and dispute resolution mechanisms. The contract can also outline performance metrics, expectations, and termination clauses if there's a non-compliance or breach.

Ongoing Monitoring and Review

Acme establishes an ongoing monitoring process to regularly assess the third party's performance and adherence to agreed-upon terms. Persons at your organization might manually perform periodic financial reviews, quality audits, site visits, or surveys. They also establish communication channels to address any concerns or changes in the third party's risk profile.

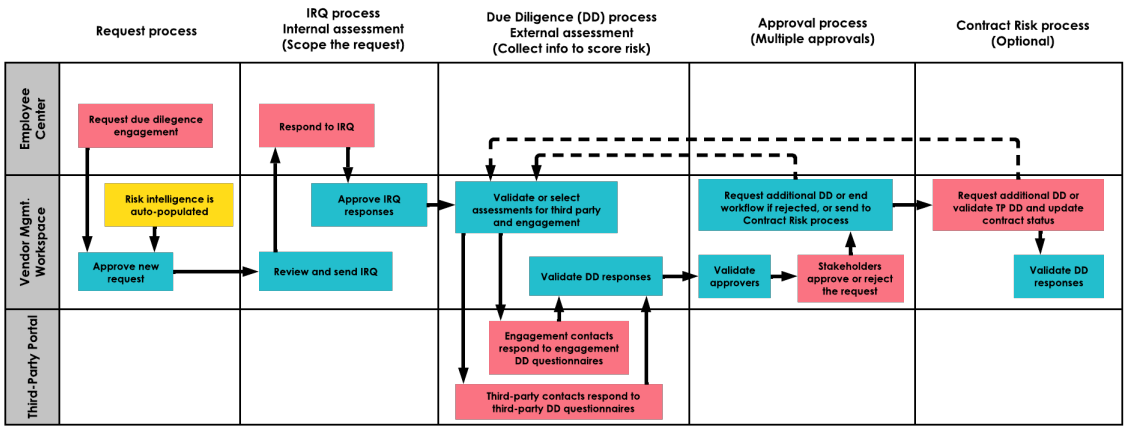
## Due diligence workflow

The Third-party risk management (TPRM) processes provide a consistent framework for your third-party risk management program. You can customize the workflow processes to meet your organization's needs.

## Processes in the due diligence workflow

Each task in a process must be completed before the next task can be started. The roles of the users that perform the various tasks are described in Roles in Third-party Risk Management. The following diagram describes the due diligence workflow.

### Due diligence workflow




Request process: Ask to start a new engagement, reassess, or offboard an existing one

1. An employee at your organization requests due diligence for a third-party engagement.
   a. The employee logs in to Employee Center on their instance. They open the due diligence request form and specify the name of the third party and the reason for the request:
      - Onboard a new engagement
      - Reassess a risk for an existing engagement
      - Reassess an existing engagement to prepare for a contract renewal
      - Offboard an engagement with due diligence
      - Offboard an engagement with no due diligence

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**b.** The employee provides details about the third party and engagement. The information includes the product or service that should be assessed in this engagement, the user who will respond to the Inherent Risk Questionnaire assessor (IRQ), and the third-party contact or engagement contact who will respond to the external questionnaires.

**c.** At any time, an external risk intelligence provider might update the risk data for the third party because a Third-party risk (TPR) manager might have integrated the services of a risk intelligence provider while configuring the application.

**d.** The employee submits the form.

**e.** The system sends out an email confirmation to the employee who made the request.

**f.** The system sends out an email notification to the Due diligence request assignment group. A member of the group can assign a TPR manager or TPR assessor to act as the owner of the request. This action triggers a task for the TPR manager.

**2.** The TPR manager scopes the request, updates it as needed, and then approves or rejects it.

**a.** The TPR manager logs in to the Vendor Management Workspace and navigates to the due diligence management page, where they review and update the request:

- The TPR manager reviews the person who was suggested as the IRQ assessor. If needed, they can specify a different person as the IRQ assessor.
- The TPR manager can start a discussion with the requester and other users by selecting **Discuss**. The message is recorded in the Activity section of the **Details** tab.

**b.** The TPR manager either rejects or approves the request. If the TPR manager accepts the request, the IRQ process starts.

**Note:** TPR assessors can create recurring third-party assessments to reassess a risk on a regular schedule. For more information, see Configure risk assessment to recur on a schedule.

IRQ process: Scope the risk

**1.** The TPR manager reviews and approves the IRQ.

**a.** In the Vendor Management Workspace, the TPR manager reviews and approves the IRQ by selecting a questionnaire that was created automatically by a business rule or from a list on the system.

The TPR administrator can create custom IRQs for an organization. The content of each IRQ is created and maintained by the person who is responsible for the business area, the geography, or third party that the questions are intended for. To define an IRQ, the TPR administrator adds sample questions to a questionnaire template and modifies the questions as needed. The sample questions are provided in the base system. Defining an IRQ is a no-code process. The TPR manager can define the business rules that auto-select the IRQ to use for an engagement.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

> **Tip:** The TPR manager can use the answer to a question in an IRQ to determine the questionnaires that are sent to the third party that is being assessed. This feature is available only if the Third-party Risk Management application has been activated.

For more information, see Create and configure an external questionnaire.

**b.** The TPR manager either rejects the due diligence request or approves it. When the request is approved, the system sends the IRQ to the IRQ assessor, which is an internal stakeholder at an organization.

**c.** The IRQ assessor is notified of the IRQ both by email and by a new task in their queue.

> **Note:** The system can also auto-send third-party risk assessments when changes to a risk score occur.

**2.** Internal users respond to the IRQ:

**a.** In the Employee Center, any user that is interested in the engagement opens and responds to the IRQ.

Several answers generate further clarifying questions. The answers can determine which external questionnaires are auto-generated and added to the set that go to the third-party contact.

For example, if an IRQ assessor responds that the third party interacts with government officials as part of the engagement, then an anti-bribery questionnaire that is appropriate to the third party's country (ABAC in the USA or FCBA in the EU, and so on) is included.

**b.** The IRQ assessor submits the completed IRQ. This action triggers a task for the TPR manager.

**3.** The internal stakeholders (third-party assessment reviewer, TPR assessor, TPR approver, TPR manager, or TPR administrator) review the IRQ responses:

**a.** In the Vendor Management Workspace, the users review the IRQ responses.

**b.** The TPR manager might ask the IRQ assessor for clarification and then either rejects or approves the IRQ responses.

**c.** If an internal stakeholder user approves the IRQ responses, they start the due diligence process by closing the engagement request.

Due diligence process: Collect information to generate a risk score

**1.** Either one of the following processes results in the selection of external due diligence questionnaires:

- In the Vendor Management Workspace, the TPR manager selects the questionnaires that the third-party contacts respond to.
- The system auto-selects the questionnaires according to the business rules that were defined to make the selections.

**2.** Regardless of the selection method that you used in step 1, two external due diligence questionnaires are selected:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- One set collects information on the third-party organization. The third-party contact responds to that questionnaire.
- The other set collects information on the business unit within the third-party organization that is the subject of the engagement. The engagement contact (as specified in the due diligence request) responds to that questionnaire.

3. In the Vendor Management Workspace, the TPR manager reviews the auto-selected questionnaires that the third-party contacts respond to. The TPR manager validates or modifies the selections and then approves the set of questionnaires.
4. The system sends out an email notification to persons at the third party. The messages notify the third-party contact and engagement contact to respond to the external questionnaires.
5. In the Third-party portal, the third-party contacts either respond to the questionnaires directly or assign the tasks to other contacts at the third-party organization.

   **Note:** The Third-party portal is fully isolated from your organization's instance.

   In an iterative process, before the TPR manager closes an assessment, the TPR manager can generate non-compliance issues and tasks. The TPR manager communicates with the TP contacts by using comments to close the issues and tasks. The TPR manager can also assign different TP contacts as needed. For more information, see Manage issues.
6. The TP contact and engagement contact return the completed questionnaires.
7. The system changes the state of the request to **Ready for TPRM approval** and sends alerts to the TPR managers.
8. In the Vendor Management Workspace, the TPR manager validates that the questionnaires are received, complete, and signed if necessary, and then closes the assessment phase to start the approval process.

Approval process: Internal stakeholder analyzes each aspect of risk

All internal stakeholders (approvers) review the questionnaire responses and supporting documents from the third-party contact. If the responses are good, one or more approvers approves and then closes the DD request. If a contract will be prepared, the approved request moves to the Contract Risk process.

- Approvers can approve or reject the request and then close it.
- Closing the request moves it either to the contract risk process, or if no contract is involved, the engagement starts.

Contract Risk process

After approval, all due diligence information can be made available for the contract negotiator. By using the Vendor Management Workspace, the contract negotiator accesses all the data that is generated during the preceding processes to design and settle the contract:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The contract negotiator can request additional due diligence if it's required.
- If the contract negotiator successfully executes a contract with the third party, they can upload it and specify the contract is executed to automatically notify all the key stakeholders.
- The contract negotiator can specify that the contract isn't executed, and the third party won't be engaged for business.
- The contract negotiator can specify that the contract is terminated, and the third party won't be engaged for business.

# Configuring Third-party Risk Management

You can activate or upgrade TPRM, by downloading the applications from the ServiceNow Store and then configuring the settings to meet your needs.

## Configuration overview

By performing the tasks in the Setup tasks for TPRM checklist, you can upgrade or install the TPRM application. After you've completed the tasks, you can perform additional configuration as described in Ongoing configuration.

## Initial setup and upgrade checklist for TPRM

Consider printing the following checklist so that you can check off the tasks as you complete them. To generate a PDF, select **Save As PDF** ( ) and then select **Selected topic**.

**Setup tasks for TPRM**

| Task | Description |
|---|---|
| ☐ | Activate the Third-party Risk Management app [com.sn_vdr_risk_asmt]. To see the instructions for downloading a GRC application from the ServiceNow® Store, see Download a GRC application from the ServiceNow Store for the first time.<br><br>**Important:** The base system includes many sample questions that you can use in your question bank. To include sample questionnaires, select **Load demo data** while installing the app.<br><br>Role required: admin |
| ☐ | Activate the Due diligence request workflow application [com.sn_tprm_dd]. To see the instructions for downloading a GRC application from the ServiceNow® Store, see Download a GRC application from the ServiceNow Store for the first time.<br><br>Role required: admin |
| ☐ | Activate the Vendor Risk Management Workspace application [sn_vrm_ws]. To see the instructions for downloading a GRC application from the ServiceNow® Store, see Download a GRC application from the ServiceNow Store for the first time.<br><br>Role required: admin |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Setup tasks for TPRM (continued)**

| Task | Description |
| --- | --- |
| ☐ | Add an authentication policy to enable secure access for external third parties. For more information, see Add an authentication policy to enable secure access for external third parties.<br><br>Role required: admin<br><br>Use the platform post-authentication policies to enable third parties to secure access to your instance. For background information on this feature, see Post-authentication context. |
| ☐ | Assign TPRM roles to users and user groups. For more information, see Assign TPRM roles to users and user groups.<br><br>Role required: admin<br><br>Assign roles to users before you implement or use the Third-party Risk Management application. Assigning roles in a well-organized manner simplifies and improves process management and helps to ensure that users are promptly notified of tasks in their areas of responsibility. |
| ☐ | Add users to groups based on their responsibilities. For more information, see Add users to groups based on responsibilities.<br><br>Role required: admin<br><br>Assign users to groups before you implement or use the Third-party Risk Management application. Each group contains users with particular roles. Well-organized user groups simplify and improve process management and help to ensure that users are promptly notified of tasks in their areas of responsibility. |
| ☐ | Configure TPRM properties. For more information, see Configure TPRM properties.<br><br>Role required: admin<br><br>Configure property settings for a variety of TPRM operations. |
| ☐ | Optional: Enable the TPRM Risk concentration map. For more information, see Enable the TPRM Risk concentration map.<br><br>Role required: admin<br><br>After you install the Risk concentration map feature, you must install a Google license to enable the feature. |
| ☐ | Enable your emails with third-party contacts. For more information, see Enable email with third-party contacts.<br><br>Role required: admin<br><br>Configure email communication with third-party contacts to enable email notification of assessments and issues. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Setup tasks for TPRM (continued)**

| Task | Description |
|---|---|
| ☐ | Optional: Import the existing data from other systems. For more information, see Import existing data from other systems.<br><br>Role required: admin<br><br>Import existing data (third parties, engagements, assessments, questionnaires, issues, and so on) from other systems (like the Aravo platform, the ProcessUnity platform, and so on). You aren't charged for importing the data. |
| ☐ | Set up third-party contacts. For more information, see Set up third-party contacts.<br><br>Role required: admin or sn_vdr_risk_asmt.vendor_risk_manager<br><br>Third-party contacts are external users at the third-party organization. They use the Third-party portal to securely organize, prioritize, and perform tasks like responding to questionnaires for assessments, performing tasks, and communicating with your risk-assessment staff regarding issues. You grant access to the Third-party portal and specify the permissions for third-party contacts. |
| ☐ | Optional: Activate a language. For more information, see Activate a language.<br><br>Role required: admin<br><br>The Now Platform uses American English by default. You can configure TPRM to use a different language. |
| ☐ | Optional: Run the quick-start tests for third-party risk management. For more information, see Run the Quick Start tests for Third-party Risk Management.<br><br>Verify that TPRM still works after you make configuration changes such as applying an upgrade or developing an application. Copy and customize the quick-start tests to pass when using your instance-specific data. |

Related topics

Ongoing configuration

## Assign TPRM roles to users and user groups

Assign roles to users before you implement or use the Third-party Risk Management application. Assigning roles in a well-organized manner simplifies and improves process management and helps to ensure that users are promptly notified of tasks in their areas of responsibility.

### Before you begin

Role required: admin

### About this task

The roles discussed in this procedure are described in Roles in Third-party Risk Management.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

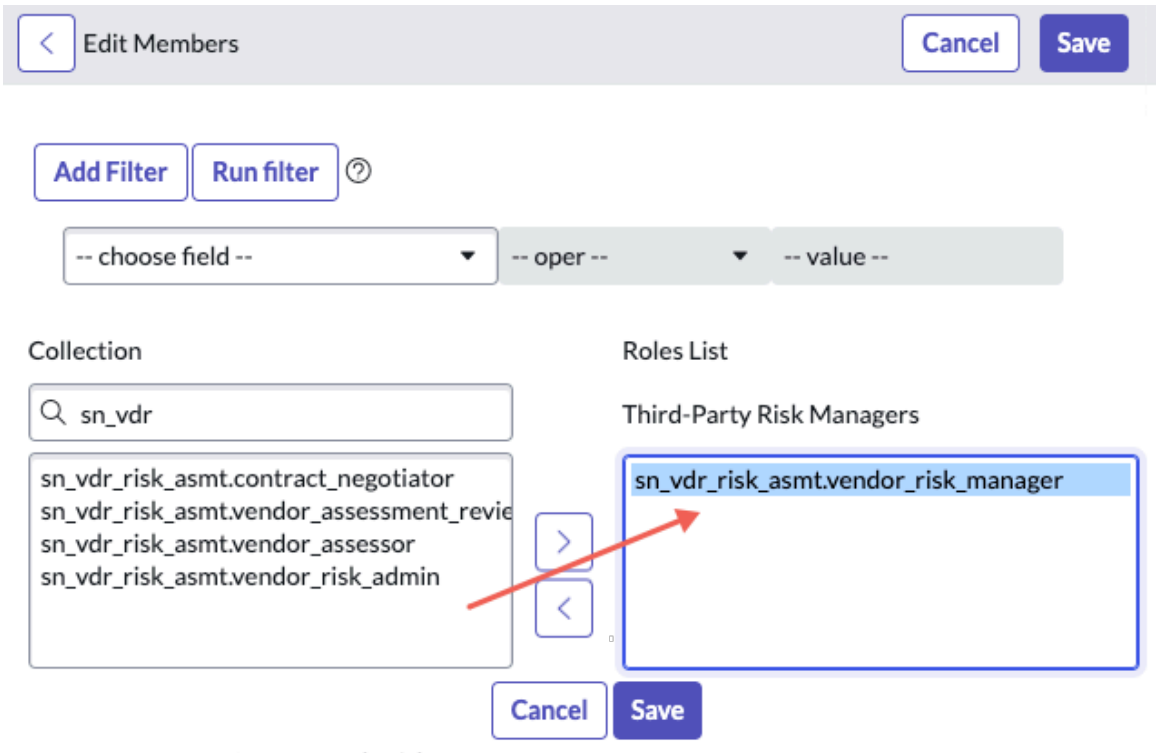
1. Navigate to **All** > **Third-party Risk Management** > **Administration** > **User Groups**.
2. Select the **Roles** related list to assign roles to the group.

   a. In the search field for the **Collection** list, enter `sn_vdr` to view the list of roles that relate to the TPRM application.

      TPRM roles are described in Roles in Third-party Risk Management.

   b. Move the roles that are appropriate for the group from the **Collection** list to the **Roles** list and then select **Save**.

      In this example, the **sn_vdr_risk_asmt.vendor_risk_manager** role is assigned to the group that the user has named `Third-party Risk Managers`.




3. On the **Group Members** related list, select **Edit**.
4. Move all appropriate users from the **Collection** list to the **Group Members List** and then select **Save**.
5. Optional: Use the **Groups** related list to add subgroups to the group that you are defining.

Related topics

- Roles in Third-party Risk Management
- TPRM and the Explicit Roles plugin

## Add users to groups based on responsibilities

Assign users to groups before you implement or use the Third-party Risk Management application. Each group contains users with particular roles. Well-organized user groups simplify and improve process management and help to ensure that users are promptly notified of tasks in their areas of responsibility.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: admin

### About this task
Several user groups are created when you activate the TPRM app. In this procedure, you add users to each group. The roles mentioned in this procedure are described in Roles in Third-party Risk Management.

There's an important practical result of including all users with a particular role in a group: Your risk management process isn't affected when one or more members of the group are unavailable due to vacation, for example.

**Important:** Consider this to be an ongoing process, where the user who is assigned as the group manager is responsible for continuously updating group membership.

Due diligence request assigners

Group members have the Third-party risk (TPR) assessor [sn_vdr_risk_asmt.vendor_assessor] role.

Each member receives email notification of new requests for due diligence. For requests in the **New** or **Unassigned** state, the **Owner** isn't yet specified. Any group member can assign the owner.

The owner is the person who owns an assessment for audit purposes and monitors and manages overall assessment processes. Owners are responsible for confirming that the assessment is completed in a timely fashion by the third party, reviewing their responses, and creating and resolving issues. To drive the assessment to its completion, owners are notified when an assessment reaches a particular milestone. The owner must have the TPR manager or TPR assessor role.

Third-party Risk Managers

Group members have both the TPR approver role [sn_vdr_risk_asmt.approver] and the TPR manager role [sn_vdr_risk_asmt.vendor_risk_manager].

Members can monitor and manage overall due diligence processes and approve new requests for due diligence.

Third-party Risk Reviewers (External assessment reviewers)

Group members have the Third-party assessment reviewer role [sn_vdr_risk_asmt.vendor_assessment_reviewer].

Members can monitor and manage interactions with third-party contacts during external due diligence processes.

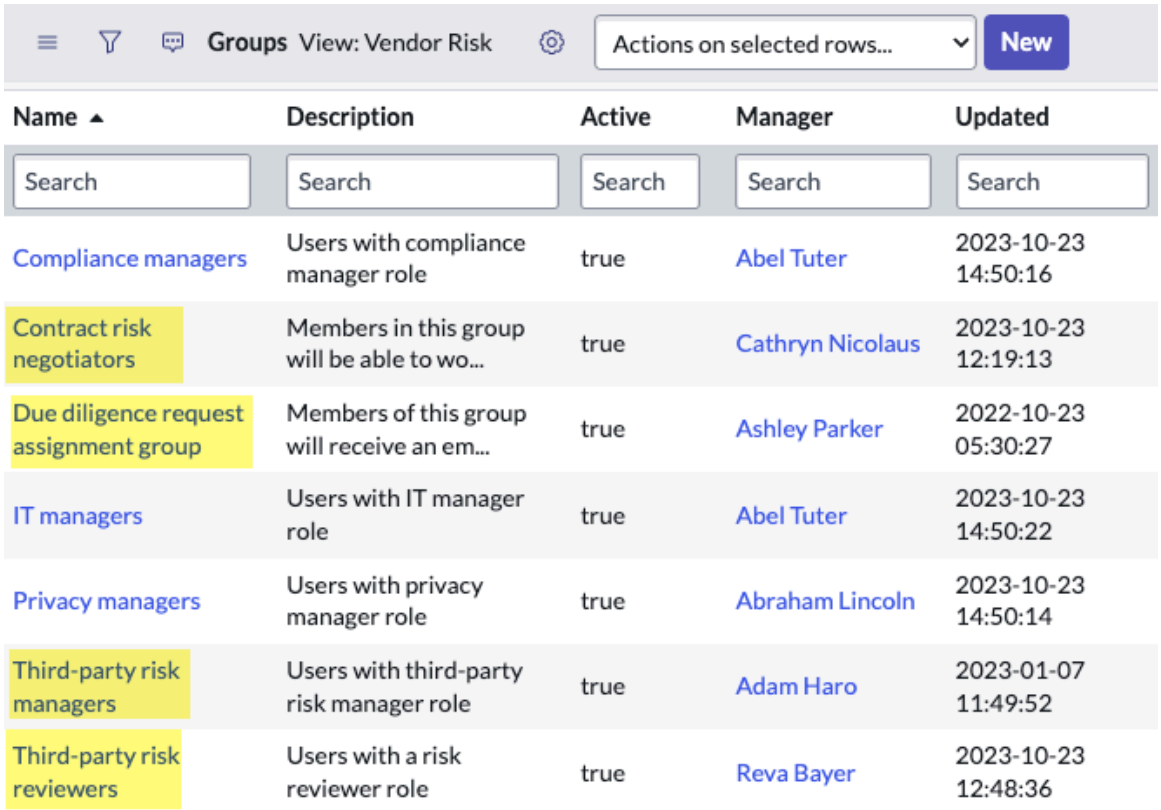
Contract risk negotiators

Group members have the Contract risk negotiator [sn_vdr_risk_asmt.contract_negotiator] role.

Members work in the contract risk process.

### Procedure
1. Navigate to **All** > **Third-party Risk Management** > **Administration** > **User Groups**.
   The list of user groups appears. In the image, TPRM groups are highlighted.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




| Name ▲ | Description | Active | Manager | Updated |
|---|---|---|---|---|
| Search | Search | Search | Search | Search |
| Compliance managers | Users with compliance manager role | true | Abel Tuter | 2023-10-23 14:50:16 |
| Contract risk negotiators | Members in this group will be able to wo... | true | Cathryn Nicolaus | 2023-10-23 12:19:13 |
| Due diligence request assignment group | Members of this group will receive an em... | true | Ashley Parker | 2022-10-23 05:30:27 |
| IT managers | Users with IT manager role | true | Abel Tuter | 2023-10-23 14:50:22 |
| Privacy managers | Users with privacy manager role | true | Abraham Lincoln | 2023-10-23 14:50:14 |
| Third-party risk managers | Users with third-party risk manager role | true | Adam Haro | 2023-01-07 11:49:52 |
| Third-party risk reviewers | Users with a risk reviewer role | true | Reva Bayer | 2023-10-23 12:48:36 |

2. Select the name of the group to update.
3. Optional: Specify a manager for the group.
   The group manager is responsible for continuously updating group membership. The group manager typically has the same role (or higher) as the members.
4. Optional: Specify an email alias for the group.
   - If you don't specify an alias, then a separate email notification is sent to each member.
   - If you specify an alias, then a single email notification is sent with all members in the **To:** list.
5. On the **Group Members** related list, select **Edit**.
6. Move all appropriate users from the **Collection** list to the **Group Members** list and then select **Save**.
7. Optional: Use the **Groups** related list to add subgroups to the group that you're defining. This option enables you to organize users into practical subsets.
8. Repeat the process for each group.

Related topics

Roles in Third-party Risk Management

TPRM and the Explicit Roles plugin

## Configure TPRM properties

Configure property settings for a variety of TPRM operations.

### Before you begin

Role required: admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

You can specify the following property settings:

The name of your organization [sn_vdr_risk_asmt.company.name]

Third-party contacts see this name in all references on the Third-party portal.

Text delimiter in spreadsheets [sn_vdr_risk_asmt.excel_choice_delimiter]

Character string that separates response text in questions of type 'Choice' and 'Multiple Selection'.

Common delimiters: \r, \n, \t, \r\n, and the comma character.

Maximum spreadsheet file size [sn_vdr_risk_asmt.excel_file_max_size]

Maximum file size in MB that can be imported.

Allow TPR assessors to modify responses in third-party questionnaires [sn_svdp.allow_assessor_edit]

You can set the following options:

- Enable TPR assessors [sn_vdr_risk_asmt.vendor_assessor] to answer questions or modify responses (default)
- Enable TPR assessors to modify responses
- Do not enable TPR assessors to answer questions or modify responses

Maximum age for reusing responses [sn_tprm_dd.max_age_for_questionnaire_reuse]

Maximum age in days for a questionnaire to be used to prepopulate responses in a new questionnaire. The questionnaire from the most recent closed assessment is used. This setting applies when a user selects the **Include previous responses** option when configuring a questionnaire or questionnaire template.

### Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Administration** > **Properties**
2. For each property, enter the value that meets your need.
   - Each property entry describes the value to enter.
   - To view the name of a property, select the information icon ( ).

## Enable the TPRM Risk concentration map

After you install the Risk concentration map feature, you must install a Google license to enable the feature.

### Before you begin

Role required: admin

### Procedure

Follow the instructions in Set up Google Maps API.

For information on the Google Maps APIs in the Geo-map component, see the KB article: KB1588661

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Enable email with third-party contacts

Configure email communication with third-party contacts to enable email notification of assessments and issues.

### Before you begin
Role required: admin

### About this task
**Note:** Third-party contacts see your organization's name in all references on the Third-party portal. You specify the name in the `sn_vdr_risk_asmt.company.name` property setting. See Configure TPRM properties.

### Procedure
1. Navigate to **All** > **System Properties** > **Email Properties**.
2. Select both the **Email sending enabled** and **Email receiving enabled** check boxes and then select **Save**.




## Import existing data from other systems

Import existing data (third parties, engagements, assessments, questionnaires, issues, and so on) from other systems (like the Aravo platform, the ProcessUnity platform, and so on). You aren't charged for importing the data.

### Before you begin
Role required: admin

### About this task
The overall process of importing data into your instance is discussed at https://docs.servicenow.com/bundle/sandiego-platform-administration/page/administer/import-sets/reference/import-sets-landing-page.html.

You will find a learning module that takes you through the process of importing data at https://developer.servicenow.com/dev.do#!/learn/courses/sandiego/app_store_learnv2_importingdata_sandiego_importing_data_into_servicenow.

A learning module on running transform maps appears at https://developer.servicenow.com/dev.do#!/learn/courses/sandiego/app_store_learnv2_importingdata_sandiego_importing_data_into_servicenow.

**Important:** To import the data without being charged, you must turn off the "Run business rules" option before running the transform map to import the data. If you do not turn off business rules, then the imported data records are marked as activity and you will be charged for a license.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Create a transform map.
   See https://docs.servicenow.com/bundle/sandiego-platform-administration/page/script/server-scripting/task/t_CreateATransformMap.html for instructions.

   **Important:** Clear the **Run business rules** check box before you run the transform map.

2. Run the transform map and repeat the process for each data set.

Related topics

Import a questionnaire from a spreadsheet

## Run the Quick Start tests for Third-party Risk Management

Verify that TPRM still works after you make configuration changes such as applying an upgrade or developing an application. Copy and customize the quick-start tests to pass when using your instance-specific data.

GRC: Vendor Manager Workspace and Third-party Risk Management quick start tests require activating the Vendor Manager Workspace and Third-party Risk Management plugin (com.sn_vdr_risk_asmt) and loading demo data.

**GRC: Vendor Risk Management and Third-party Risk Management Quick Start Tests**

| Test | Description |
|---|---|
| GRC: Create Engagement Risk Assessment | Creates and submits an engagement risk assessment to an engagement. |
| GRC: Vendor Risk Scoring - Cancel assessment for engagement | Verifies a request to recalculate a risk rating is automatically created on an Engagement and Third party after one assessment for the Engagement is cancelled. |
| GRC: Vendor Issue ATF | Creates and submits a third-party risk issue form and third-party risk task form. |
| GRC: Create Vendor Risk Assessment | Creates and submits a vendor risk assessment to a vendor. |
| GRC: Vendor Portal - Answer and Return Assessment | Vendor contact answers and submits assessment in the Service Vendor Portal. |
| GRC: Vendor Tiering Assessment | Selects and submits an assessment to respective assessors after changing the duration. |

Related topics

Quick start tests

## Event-driven management — automate external assessment processes

Use the Event-driven management feature to configure rules that auto-generate and send questionnaires and doc requests to engagements and third parties. For engagements and third parties that meet criteria you define, you specify the schedule and the assessment templates. You can automate all assessment types except onboarding.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_vdr_risk_asmt.vendor_risk_manager

### Procedure
1. Use either of the following methods to start the process:
   - Workspace: Select **Workspaces** > **Vendor Management Workspace**. On the **Risk** tab, select the list icon  . In the **Event-driven management** list, select any option: **Active**, **Inactive**, or **All**.
   - Legacy: Navigate to **All** > **Third-party Risk Management** > **Event-driven management** and then select any option: **Active**, **Inactive**, or **All**.
2. Select **New** and then fill in the form.

   The following settings appear in sections on the workspace page and as related lists on the legacy form.

#### Event-driven management rule form

| Field | Description |
|---|---|
| Name | Meaningful name for the rule that helps others understand its intent and operation. |
| Number | For each Event-driven management rule, the system auto-assigns a unique ID number that starts with the text **EMR**. In the history table of rule runs (executions), the system auto-assigns a unique ID number for each run that starts with the text **EMH**.<br><br>The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Business justification | The business reason for defining the automated process. |
| Technical description | The conditions that trigger the run and the kinds of third parties that are affected. |
| **Scope**: Specify the kind of assessment to generate and the template to use. | |
| Category | ◦ External assessment: Send questionnaires and doc requests. In the **Applies to** field, you specify whether to send the materials to third parties or to engagements.<br>◦ Reassess engagement: Reassess an existing engagement when the conditions change. For example, let's say that you hear adverse news or have changes in your third-party's supply lines. You might want to reassess the risk by conducting additional due diligence.<br>◦ Reassess engagement for contract renewal: Reassess the risk before your |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

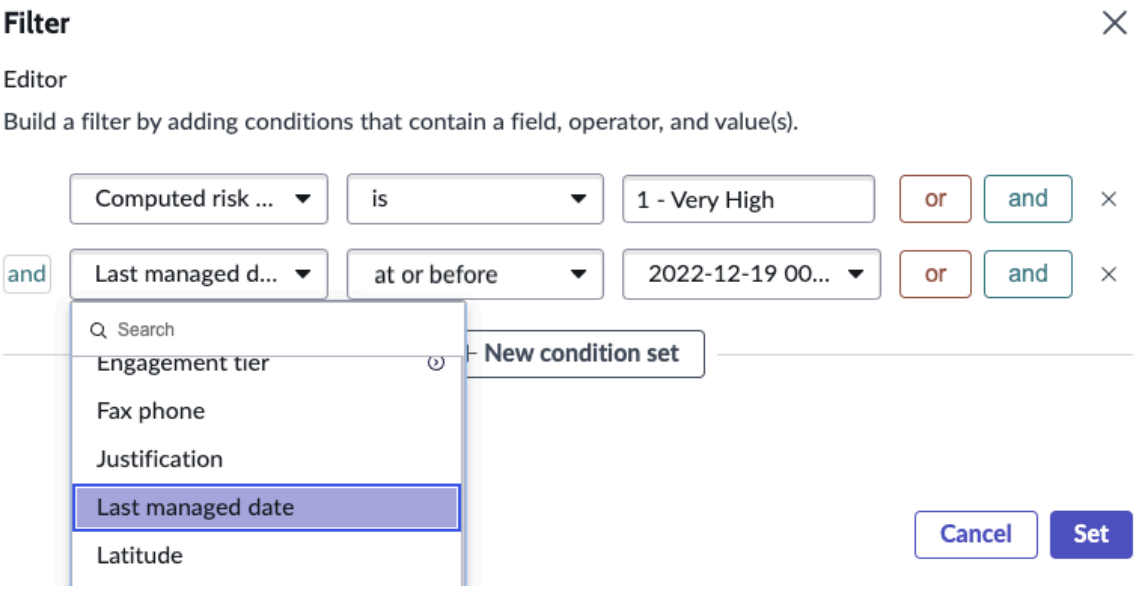
| Field | Description |
| --- | --- |
| | organization renews the contract with a current third party or engagement by conducting due diligence.<br>◦ Offboard engagement with due diligence: Determine if offboarding (terminating the relationship) with an engagement is the optimal course of action by conducting due diligence. For example, it might be too risky to switch third parties or engagements even if their current performance doesn't meet expectations.<br>◦ Offboard engagement with NO due diligence: Request that an engagement be permanently terminated when an engagement ends or you want to switch to a different third party for other reasons. In this case, you typically don't need to conduct additional due diligence. The process does, however, include the normal Inherent Risk Questionnaire (IRQ) process to confirm that the services provided by the engagement will no longer continue. For important details, see Offboarding an engagement without conducting due diligence. |
| Applies to | This field is editable only if you set the category as **External assessment**.<br>Specify whether the questionnaires and doc requests should be sent to third parties or to engagements. |
| IRQ template | This field appears if you select any category other than **External assessment**.<br>Template that specifies the contents of the Inherent Risk Questionnaire (IRQ). |
| Assessment template | This field appears only if you set the category as **External assessment**.<br>Template that specifies the questionnaires and doc requests to send. |
| **Run options**: Define the trigger and the schedule for generating the assessments. | |
| Run type | Specify how the rule should be triggered. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ **One-time**: Send the third-party risk assessment on the date that you specify in the **Start date** field.<br>◦ **Recurring**: Send the third-party risk assessment on the schedule that you specify with the **Frequency** setting.<br>◦ **On-demand**: The rule runs only when a user selects **Run now**.<br>**Note:** Regardless of the **Run type** setting, you can select **Run now** at any time to run the rule immediately. Such an on-demand run doesn't affect future scheduled runs. In the run history, the **Trigger action** for the run is recorded as **Manual**. |
| Frequency | This field appears only if you select the **Recurring** run type.<br>Specify how often the rule should run. |
| Start date | This field appears only if you select the **Recurring** or **One-time** run type.<br>First date that an active rule is available to run (depending on the specified filter conditions). A one-time rule runs on the start date. |
| End date | This field appears only if you select the **Recurring** run type.<br>Last date that an active rule is available to run (depending on the specified filter conditions). A rule becomes inactive after the end date.<br>If you don't specify an end date, then the rule continues until you delete or update it. |

3. Specify the filter conditions.
   Use the filter editor to specify the conditions that determine which third parties or engagements should receive the questionnaires and doc requests.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




When you select **Set**, the system applies the filter and displays a link to enable you to view the list of engagements or third parties that match the filter conditions.

4. Specify how the Third-party Risk (TPR) assessor [sn_vdr_risk_asmt.vendor_assessor], owner, and contract risk negotiator [sn_vdr_risk_asmt.contract_negotiator] are selected for the engagements or third parties that match the filter conditions.

| Option | Description |
|---|---|
| Use last | Assign the user that most recently performed the function for the engagement. |
| Use onboarding | Assign the user that most recently performed the function during onboarding for the engagement. |
| Specify now | When you select this option, a selection box opens to enable you to specify the user. |
| Specify later | When you select this option, after the rule is saved, you or another user can specify the appropriate TPR assessor or contract risk negotiator later during the workflow. This option doesn't appear for owner selection. |

5. Select **Save** in the workspace or **Submit** in the form.
   - The system saves the rule.
   - Regardless of the **Run type** setting, you can select **Run now** at any time to run the rule immediately. Such an on-demand run doesn't affect future scheduled runs. In the run history, the **Trigger action** for the run is recorded as **Manual**.
   - The system displays the following additional read-only values on the workspace **Details** tab and on the form.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Additional values

| Field | Description |
|---|---|
| Active | Option to activate the rule. By default, newly defined rules aren't active.<br>◦ Only active rules with a **Run status** value of **Ready** can run when the specified conditions are met.<br>◦ You can, however, run a rule configured as **On-demand** whether it's active or not. |
| Run status | ◦ **Ready**: The rule is defined and can run as determined by the filter conditions and schedule.<br>**Note:** Only active rules with a **Run status** value of **Ready** can run when the specified conditions are met.<br>◦ **Running**: The rule is currently running (questionnaires and document requests are being sent). For rules that are currently running: The duration between the **Run start** timestamp and the current time indicates how long the rule has been running.<br>**Note:** Regardless of the **Run type** setting, you can select **Run now** at any time to run the rule immediately. Such an on-demand run doesn't affect future scheduled runs. In the run history, the **Trigger action** for the run is recorded as **Manual**.<br>If a rule seems to be stuck running for an excessive time:<br>**a.** Go to **Process automation** > **Flow Administration** > **Event Queue**.<br>**b.** Find the platform background task with a name that starts with `sn_vdr` or `sn_tprm` that is in the **error** state. |
| Next scheduled run | For rules with a recurring **Run type**, the read-only date of the next scheduled run is calculated based on the specified filter conditions and the **Frequency** setting. |
| Last successful run | Timestamp of the most recent run that is in the **Successful** state. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Related topics

View the run history for event-driven management rules

### View the run history for event-driven management rules

When an event-driven management rule runs, it auto-generates and sends questionnaires and doc requests to third parties. You can view the current state (running, successful, or recalled) of all runs of rules. Select a record number to view details and to view the set of assessments generated by the rule.

## Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager

## Procedure

1. Use either of the following methods to start the process:
   - Workspace: Select **Workspaces** > **Vendor Management Workspace**. On the **Risk** tab, select the list icon  . In the **Event-driven management** list, select any option: **Active**, **Inactive**, or **All**.
   - Legacy: Navigate to **All** > **Third-party Risk Management** > **Event-driven management** and then select any option: **Active**, **Inactive**, or **All**.
2. Select the **Event-driven management history** tab in the workspace or view the **Event-driven management history** related list on the form.

   Each record of a run includes the following read-only values:

**Event-driven management history**

| Field | Description |
|---|---|
| Number | Select a number to view the **Details** tab for the run.<br><br>For each Event-driven management rule, the system auto-assigns a unique ID number that starts with the text **EMR**. In the history table of rule runs (executions), the system auto-assigns a unique ID number for each run that starts with the text **EMH**.<br><br>The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Trigger action | ◦ **Scheduled job**: The rule ran on the schedule specified for the **Frequency** setting.<br>◦ **Manual**: The rule ran when a user selected **Run now**. |
| Run start | Date and time that the rule started to run.<br><br>For rules that are currently running: The duration between the **Run start** timestamp |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | and the current time indicates how long the rule has been running. |
| Run complete | Date and time that the rule ended a run. |
| State | ◦ **Running**: The rule is currently running (questionnaires and document requests are being sent). For rules that are currently running: The duration between the **Run start** timestamp and the current time indicates how long the rule has been running.<br>◦ **Successful**: The rule ran to completion and sent all questionnaires and doc requests to third parties.<br>◦ **Recall in progress**: The rule was recalled and is currently removing questionnaires and document requests from Third-party portals.<br>◦ **Recalled**: After the rule completed the run, a user recalled the third-party risk assessments. See Recall event-driven questionnaires and doc requests. |

### View the assessments generated by event-driven management rules

When an event-driven management rule runs, it auto-generates and sends questionnaires and doc requests to third parties. You can view the current state (running, successful, or recalled) of all runs of rules. Select a record number to view details and to view the set of assessments generated by the rule.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager

### Procedure

1. On the Vendor Management Workspace, use either of the following methods to start the process:

   ◦ To view all DD requests and assessments for a particular rule:

   a. Select the list icon .
   b. In the **Event-driven management rules** list, select any option: **Active**, **Inactive**, or **All**.
   c. In the **Event-driven management** list, select any option: **Active**, **Inactive**, or **All**.
   d. Select a rule.
   e. On the **Event-driven management history** tab, select a run.
   f. Select the appropriate tab to view the DD requests or assessments that the rule sent.

   ◦ To view the DD requests and assessments for a particular run of a rule:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Select the list icon  .

b. In the **Event-driven management** list, select either option: **Successful runs** or **Recalled runs**.

c. Select a run.

d. Select the appropriate tab to view the DD requests or assessments that the rule sent.

2. On the legacy interface, use the following method:

◦ To view the DD requests and assessments for a particular run of a rule:

a. Navigate to **All** > **Third-party Risk Management** > **Event-driven management** and then select either option: **Successful runs**, **Recalled runs**.

b. Select a run.

c. Select the appropriate tab to view the DD requests or assessments that the rule sent.

3. Select the **Details** tab to view the record of a run.

Each record includes the following read-only values:

**Event-driven management history**

| Field | Description |
|---|---|
| Number | For each Event-driven management rule, the system auto-assigns a unique ID number that starts with the text **EMR**. In the history table of rule runs (executions), the system auto-assigns a unique ID number for each run that starts with the text **EMH**.<br><br>The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Trigger action | ◦ **Scheduled job**: The rule ran on the schedule specified for the **Frequency** setting.<br>◦ **Manual**: The rule ran when a user selected **Run now**. |
| Run start | Date and time that the rule started to run.<br><br>For rules that are currently running: The duration between the **Run start** timestamp and the current time indicates how long the rule has been running.<br><br>If a rule seems to be stuck running for an excessive time:<br>**a.** Go to **Process automation** > **Flow Administration** > **Event Queue**.<br>**b.** Find the platform background task with a name that starts with `sn_vdr` or `sn_tprm` that is in the **error** state. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Run complete | The date and time that the rule ended a run. |
| State | ◦ **Running**: The rule is currently running (questionnaires and document requests are being sent). For rules that are currently running: The duration between the **Run start** timestamp and the current time indicates how long the rule has been running.<br>◦ **Successful**: The rule ran to completion and sent all questionnaires and doc requests to third parties.<br>◦ **Recalled**: After the rule completed the run, a user recalled the questionnaires and document requests. See Recall event-driven questionnaires and doc requests. |

### Recall event-driven questionnaires and doc requests

You can recall third-party risk assessments (questionnaires and document requests) that were sent by an event-driven management rule. The items are removed from Third-party portal for all third parties or engagements that haven't yet responded.

#### Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager

#### About this task

**Important:** The questionnaires and document requests are removed from the Third-party portal only for third parties where no item had yet been returned.

#### Procedure

1. Use either of the following methods to start the process:
   - Workspace: Select **Workspaces** > **Vendor Management Workspace**. On the **Risk** tab, select the list icon  . In the **Event-driven management** list, select any option: **Active**, **Inactive**, or **All**.
   - Legacy: Navigate to **All** > **Third-party Risk Management** > **Event-driven management** and then select any option: **Active**, **Inactive**, or **All**.
2. Enter text that explains the reason for recalling the items in the **Recall justification** field and then select **Recall**.

   The third-party risk assessments are removed from the affected Third-party portals and the **State** value of the rule is set to **Recalled**.

## Ongoing configuration

The TPR manager and TPR admin roles involve a broad variety of responsibilities. After the TPRM base system is set up, you configure additional settings that enable and enhance everyday risk-assessment tasks.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## TPR management processes

### Set up risk rating scales and scoring

The risk rating scale helps business users better understand risk assessment results. For example, in the default settings, risk scores in the 20 through 39 range indicate high risk, while scores in the 60 through 79 range indicate low risk.

**Note:** Many organizations find that the default settings represent their needs appropriately and don't change the settings.

Role required: admin or sn_vdr_risk_asmt.vendor_risk_manager.

### Create and configure an external questionnaire

As part of any due-diligence process, you send multiple questionnaires and possibly document requests to the third-party contact. To simplify this ongoing task, you define questionnaire templates and document-request templates and then group them into reusable assessment templates.

Role required: admin or sn_vdr_risk_asmt.vendor_risk_admin for questionnaire and document request templates and sn_vdr_risk_asmt.vendor_risk_manager for assessment templates.

## Configure TPR management processes

Set up business rules to auto-select the appropriate IRQ for a request for due diligence.

### Set up the approval levels for due diligence requests

Set up rules at each approval level by selecting an approver type and the number of required approvals. You can additionally filter conditions on the table to which each approval rule is applied to help ensure that the correct individual is assigned as an approver.

Role required: admin or sn_vdr_risk_asmt.vendor_risk_admin

### Set up the approval rules for due diligence requests

Set up rules at each approval level by selecting an approver type and the number of required approvals. Define filter conditions on the Third-party due diligence request table to which each approval rule is applied.

Role required: admin or sn_vdr_risk_asmt.vendor_risk_admin

**Note:** For more information about the Approver Configurator application, see Approval configuration.

#### Set up risk rating scales and scoring

The risk rating scale helps business users better understand risk assessment results. For example, in the default settings, risk scores in the 20 through 39 range indicate high risk, while scores in the 60 through 79 range indicate low risk..

**Before you begin**
Role required: admin or sn_vdr_risk_asmt.vendor_risk_manager

**About this task**

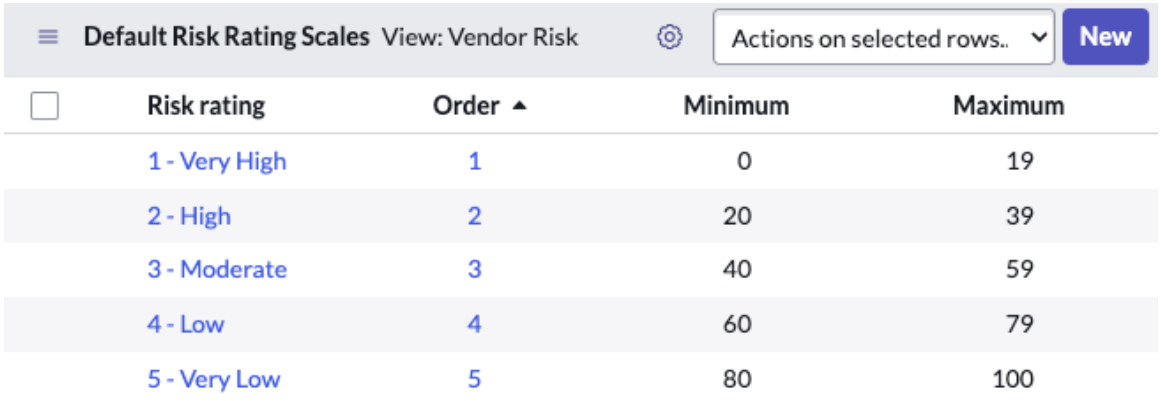
**Note:** Many organizations find that the default settings represent their needs appropriately and don't change the settings.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

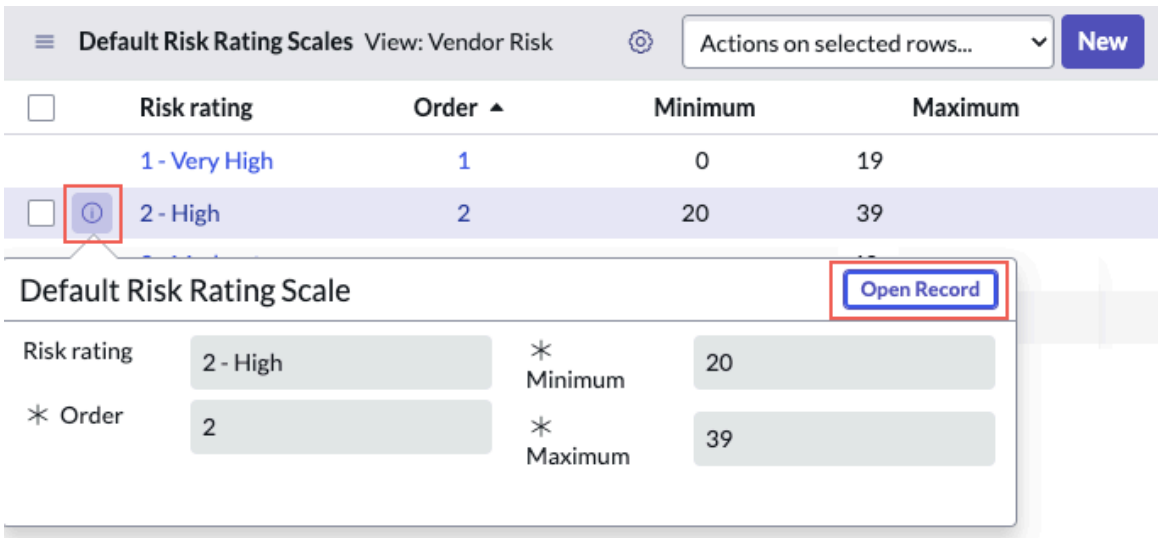
## Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Assessment Setup** > **Risk Rating Scale** to modify or refine the Risk Rating Scale.

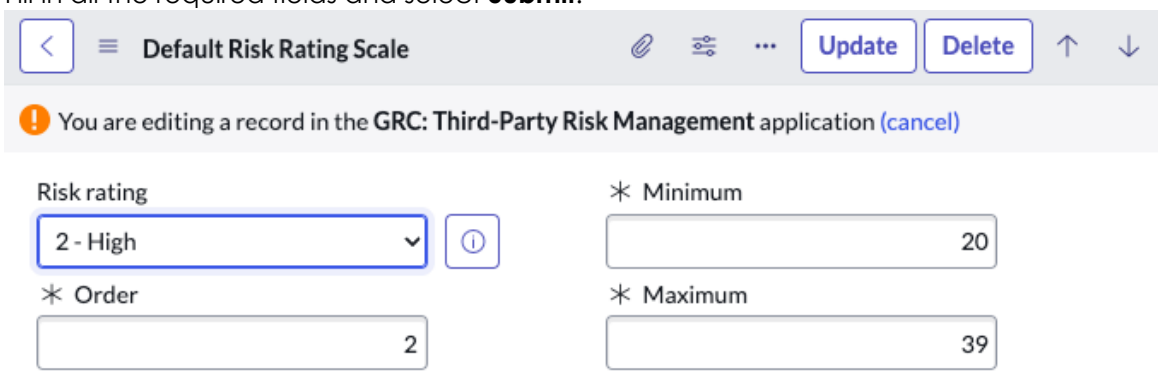
   The base system includes five ratings. You can customize their maximum and minimum values.




2. Refine the values.
   Select the **Information** icon to preview the **Risk Rating Scale** value. Select the **Open Record** in the pop-up.




3. Fill in all the required fields and select **Submit**.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Define third-party risk scoring rules

Define criteria, based on risk scores, that determine which third parties require assessments. Third-party risk scoring rules apply to subsidiaries and engagements and to third-party risk areas.

## Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager

## About this task

## Procedure

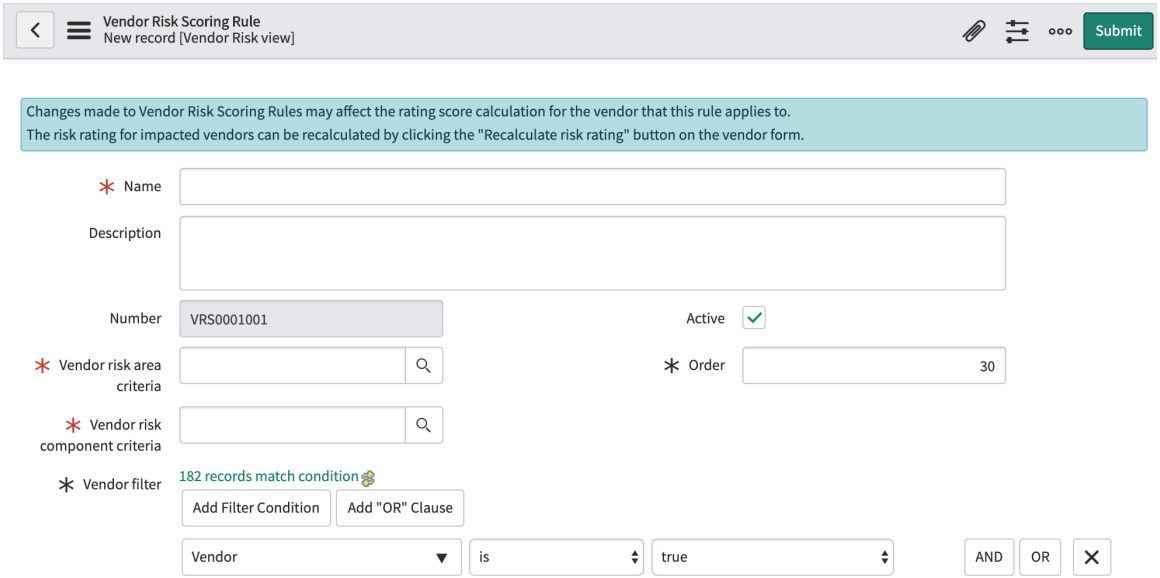
1. Navigate to **All** > **Third-party Risk Management** > **Scoring Setup** > **Third-party Risk Scoring Rules**.
2. Select **New**, fill in the form, and then select **Submit**.

### Third-party Risk Scoring Rule form

| Field | Description |
|---|---|
| Name | Name of the scoring rule. |
| Description | Description of the scoring rule that will help other users understand its intent. |
| Number | For each third-party risk scoring rule, the system auto-assigns a unique ID number that starts with the text **VRS**.<br><br>The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Third-party risk area criteria | The risk area criteria that applies to this engagement risk scoring rule.<br><br>A third-party risk area criteria is a group of risk domains (sometimes called risk areas in other platform features) that applies to a particular type of third party. See Define third-party risk area criteriafor details on how the criteria are defined. |
| Third-party risk component criteria | Criteria for third-party risk assessments, engagements, and subsidiaries that applies to this risk scoring rule.<br><br>Components are the entities for which you can assess risk (for example, subsidiaries or engagements). A component criteria is a group of components that should apply to a particular type of third party.<br><br>See Define component criteria. |
| Active | Option to activate the rule. Only active rules are applied. |
| Order | Select the order to indicate the rule's precedence. If multiple rules apply to the same third-party risk area, engagement, or subsidiary, the one with the higher-order value is applied. |
| Vendor filter | Use the condition builder to define the rules for selecting third parties. For example, you can filter on third parties with whom you do considerable |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | business (Size is $1,000,000) or third parties within a specific category (Category is software). |




## What to do next

Continue with the checklist of required setup procedures.

### Define engagement risk scoring rules

An engagement risk-scoring rule specifies component criteria that determine which engagements are selected for assessment. For example, a rule could enable assessments for engagements that involve more than $40,000 annual business. Engagement scoring rules apply only to engagements.

## Before you begin

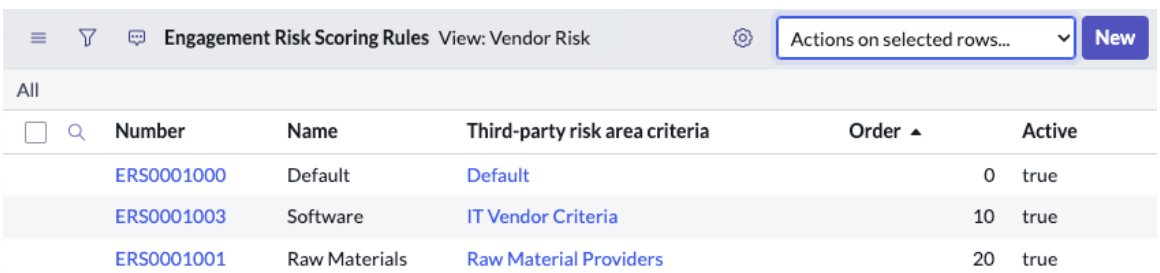
Role required: sn_vdr_risk_asmt.vendor_risk_manager

## About this task

**Important:** Engagement risk scoring rules apply only to engagements and not to parent third parties. Engagement risk rating scores, therefore, apply only to risk assessments for the engagement.

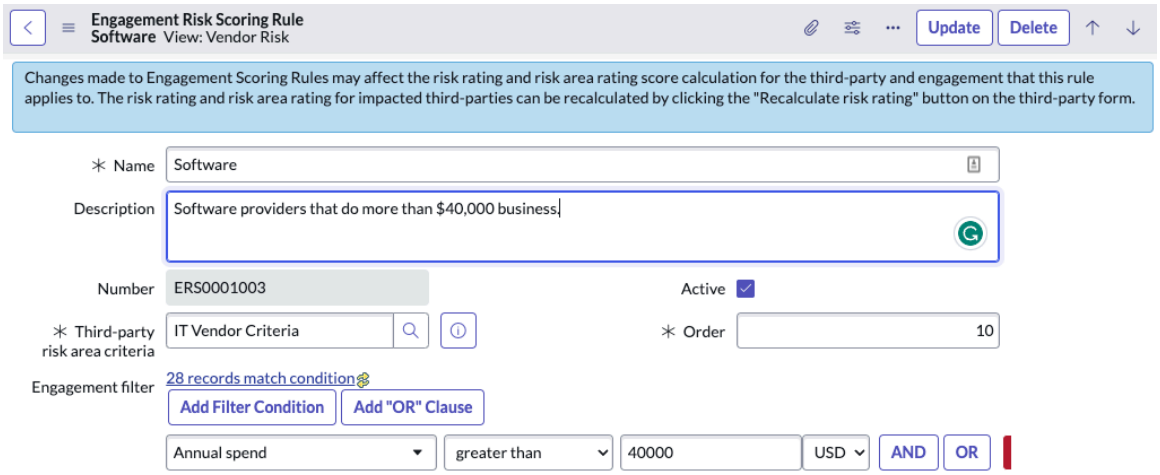
## Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Scoring Setup** > **Engagement Risk Scoring Rules**.




2. Select **New**, fill in the form, and then select **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




### Engagement Risk Scoring Rules form

| Field | Description |
|---|---|
| Name | Name of the scoring rule. |
| Description | Description of the scoring rule. |
| Number | For each engagement risk scoring rule, the system auto-assigns a unique ID number that starts with the text **ERS**.<br><br>The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Vendor risk area criteria | The risk area criteria that applies to this engagement risk scoring rule.<br><br>A third-party risk area criteria is a group of risk domains (sometimes called risk areas in other platform features) that applies to a particular type of third party. See Define third-party risk area criteria for details on how criteria are defined. |
| Active | Option to activate the rule. Only active rules are applied to engagements. |
| Order | Specify the order to indicate the rule's precedence. If multiple rules apply to the same engagement, the one with the higher-order value is applied. |
| Engagement Filter | Criteria for selecting engagements.<br><br>Use the condition builder to define the criteria.<br><br>For example, you can perform assessments for third parties with whom you do considerable business: `Annual spend is greater than $40,000` or third parties within a particular category: `Category is software`. |

## What to do next

Continue with the checklist of required setup procedures.

### Define component criteria

Components are the entities for which you can assess risk (for example, subsidiaries or engagements). A component criteria is a group of components that should apply to a particular type of third party.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_vdr_risk_asmt.vendor_risk_manager

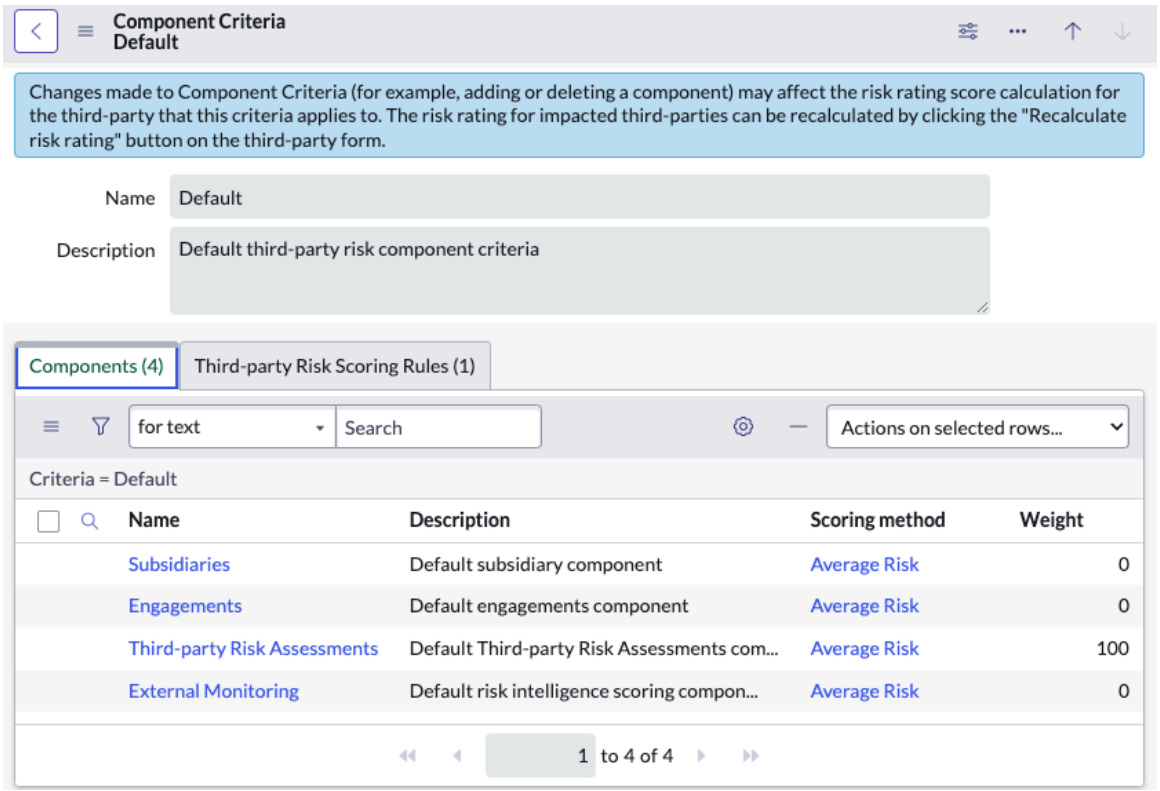
### About this task
Components are the entities for which you can assess risk. The base system comes with three components:

- Third-party risk assessments (External risk assessments)
- Subsidiaries
- Engagements

You can view the components by navigating to **Third-party Risk Management** > **Scoring Setup** > **Components**.

**Note:** You can't add new components or modify existing ones. You can, however, define the criteria (in terms of scoring method and weight) to be used to assess the components. You can update the **Default scoring method** to specify how multiple scores for each risk area are calculated. You can use the **Default weight** to adjust the weight of third-party provider scores in the third party's overall risk rating.

### Procedure
1. Navigate to **Third-party Risk Management** > **Scoring Setup** > **Component Criteria**.
2. Select the **Default** entry to open the default criteria.




3. Based on the amount of emphasis your company places on each of the component types, open each component and assign a weight.

   For example, you could create component criteria for all IT third parties and care most about third-party risk assessments, as follows:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Example: Assigning weight to component for IT third parties

| Component | Weight |
|---|---|
| Child Vendors | 5 |
| Engagements | 5 |
| External Risk Assessments | 90 |

4. When you have finished assigning weights, select **Update**.

## What to do next
Continue with the checklist of required setup procedures.

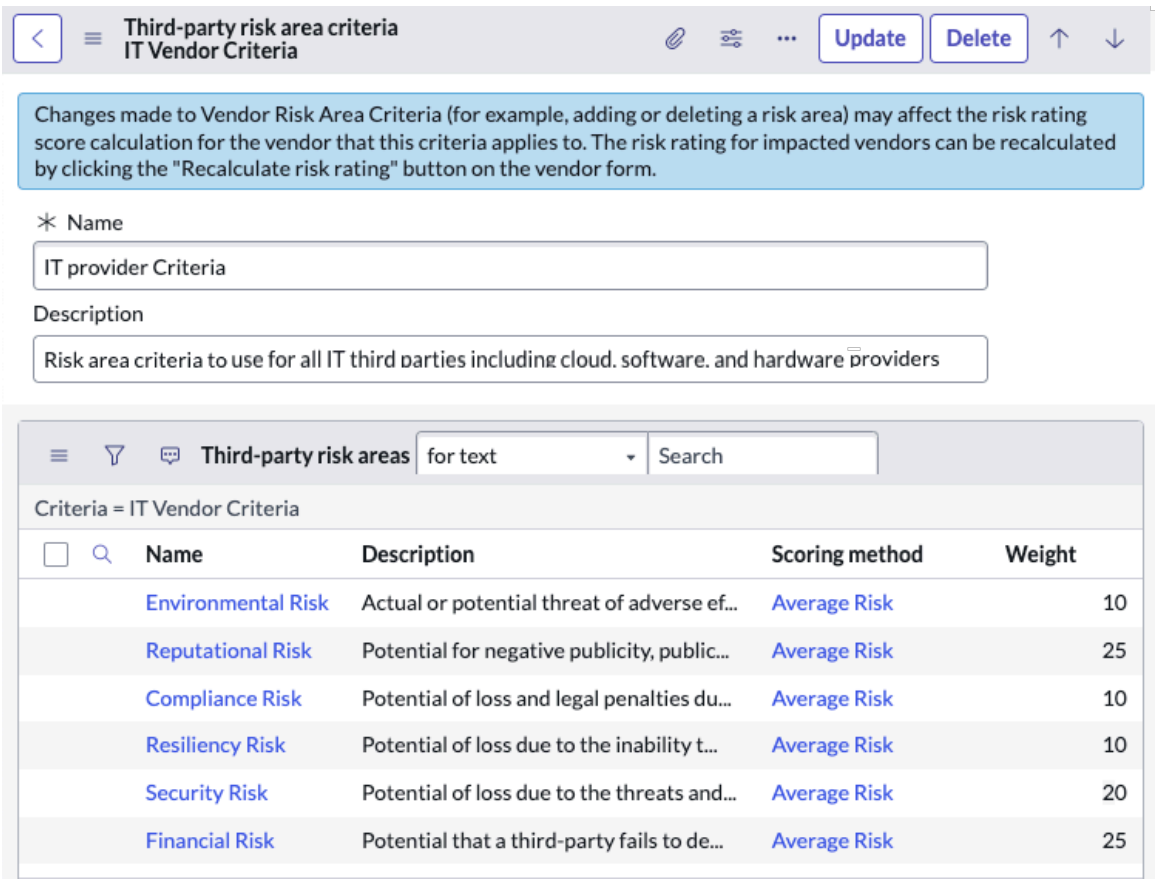
### Define third-party risk area criteria

A third-party risk area criteria is a group of risk domains (sometimes called risk areas in other platform features) that applies to a particular type of third party.

## Before you begin
Role required: sn_vdr_risk_asmt.vendor_risk_manager

## About this task
This is an example of the group of risk domains that you include in a risk area criteria that you might apply to IT service providers.

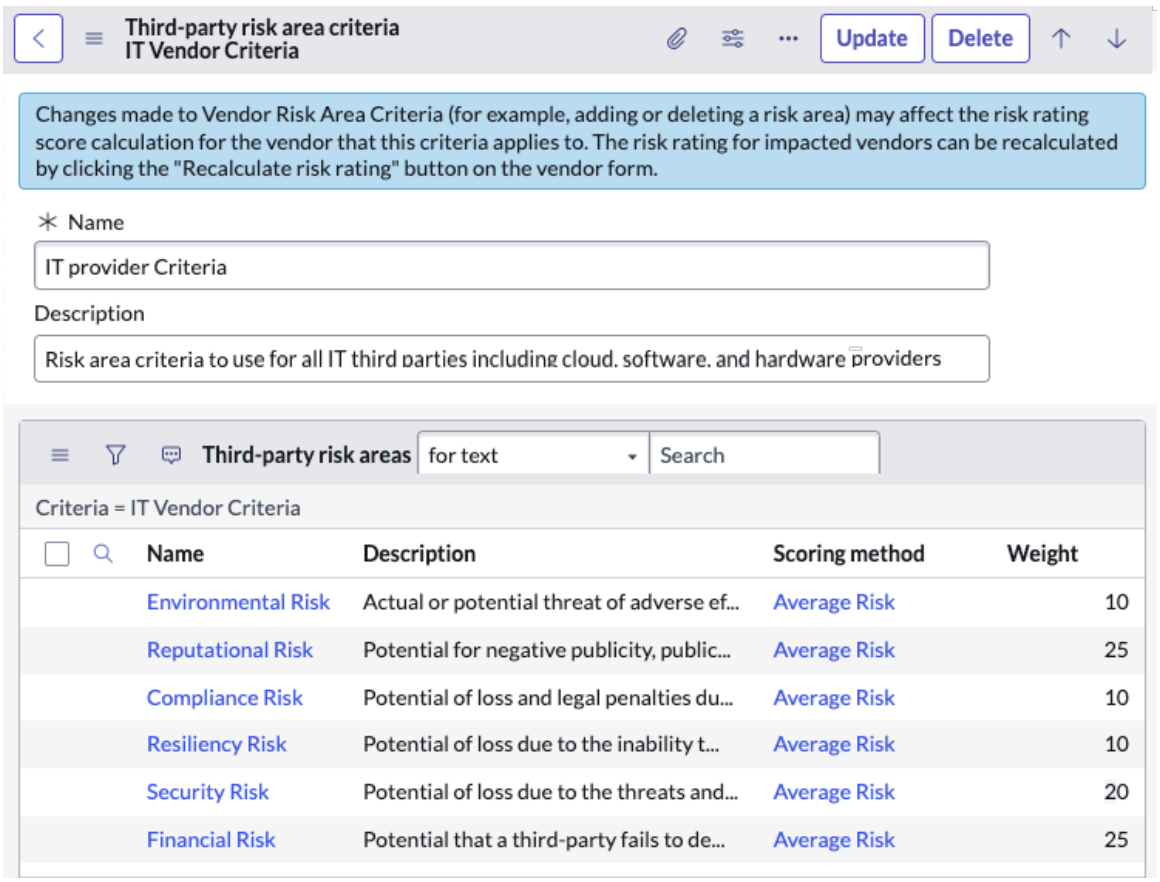
**Note:** Risk domains are called "risk areas" in some platform applications.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

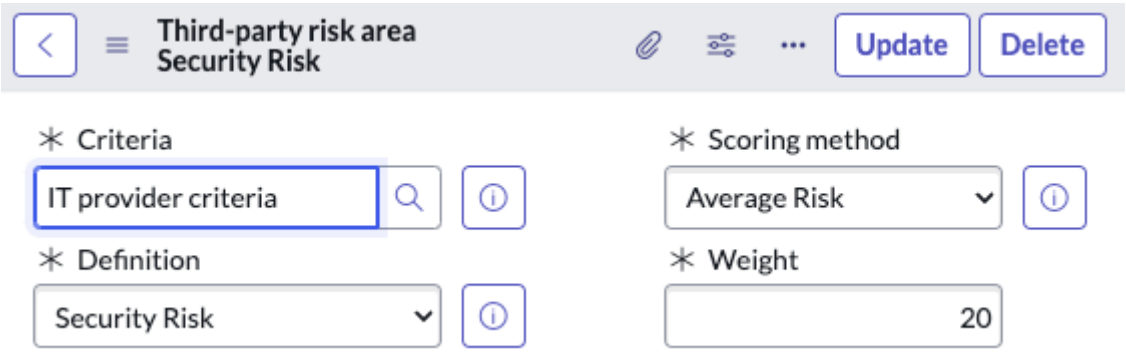
1. Navigate to **All** > **Third-party Risk Management** > **Scoring Setup** > **Risk Domain Criteria**.
2. Select **New**, enter a **Name** and **Description**, and then save the record.
   The **Third-party Risk Areas** related list appears. In the following steps, you specify the risk areas to include in the risk area criteria.
3. On the **Third-party Risk Areas** related list, select **Edit**.
4. On the Edit Members page, select the third-party risk areas to add to the third-party risk area criteria record and then select **Save**.
   - The selected third-party risk areas appear in the **Third-party risk areas** related list.
   - Scoring method and weight are copied from the risk areas.
   - You can adjust the weight of each risk area within a criteria definition.
   - You can override the values when needed.




5. Optional: To edit **Scoring method** and **Weight**, select the name of a third-party risk area.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Important:** Changes to the scoring method and weight are used for the third-party risk area criteria record but aren't saved in the individual risk area definition records.




**Example:**
Assume you're creating a third-party risk area criteria with two risk areas: Financial and Security. Financial has a scoring method of Min Risk and a weight of 10.

- Your company is more concerned with security-related criteria, so the Security risk area has a scoring method of Average Risk and a weight of 20.
- The weights for both risk areas add up to 30. So the risk area with a weight of 10 calculates as 10/30 or roughly 33%.
- The risk area with a weight of 20 calculates as 20/30 or roughly 66%.
- If both risk areas had a weight of 10, they would each carry a weight of 50%.

### What to do next
Continue with the checklist of required setup procedures.

## Define a third-party risk domain

A risk domain defines the type of risk to assess for a third party. For example, you might want to assess a data-management third party in terms of security risk and a bank in terms of financial risk. Security risk and financial risk are risk domains. Some platform applications refer to risk domains as "risk areas."

### Before you begin
Role required: sn_vdr_risk_asmt.vendor_risk_manager

### About this task
**Note:** Risk domains are called "risk areas" in some platform applications.

You can better understand and mitigate the risks that a third party poses to your organization by identifying the domains of their business to assess for risk and quantifying the importance (weight) of each domain.

- Security risk domain: A third party that handles sensitive personal data in their infrastructure might need to be assessed against their security posture.
- Reputational risk domain: If that personal data were breached, it could cause damage to your reputation due to negative media attention.
- Financial risk domain: If a third party fails to deliver on time, you might have to pay fines, settlements, or both resulting in financial loss.

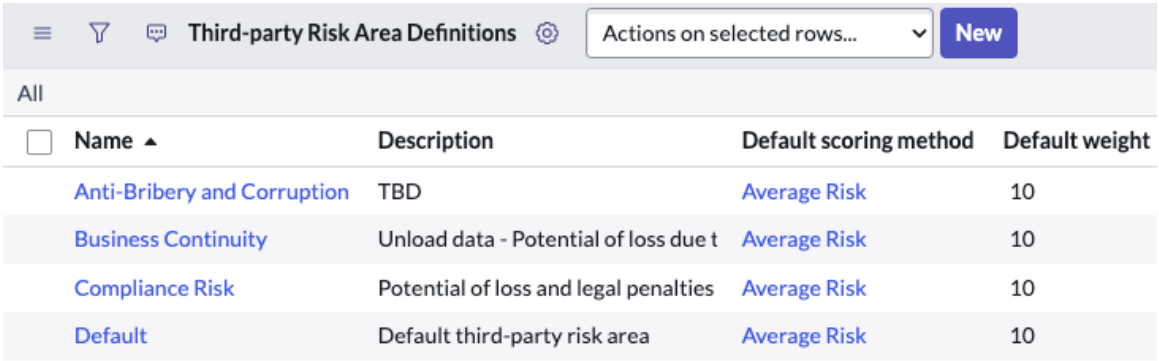
In this procedure, you create a Risk domain definition. In each definition, you specify the criteria that determine which organizations should be assessed for a particular type of risk.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** Risk domain definitions are called Risk area definitions on the forms.

### Procedure

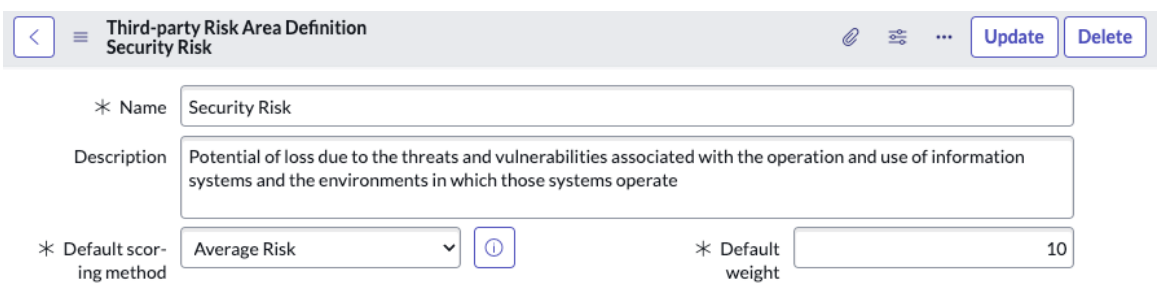
1. Navigate to **All** > **Third-party Risk Management** > **Scoring Setup** > **Risk Domains**.




2. Select **New**, fill in the form, and then select **Submit**.

#### Third-party Risk Area Definition form

| Field | Description |
|---|---|
| Name | Name of the risk domain. |
| Description | A description of the risk domain that helps colleagues to understand the intent of the definition. See the example. |
| Default scoring method | The default scoring method for third parties in this risk domain. The scoring methods are based on how well a third-party contact answers 100 questions:<br>◦ Average Risk: A rounded average of the ratings earns an Average Risk (Moderate) for the third party.<br>◦ Max Risk: A score of 0 indicates that all questions were answered incorrectly and the risk for that third party would be Max Risk (Critical).<br>◦ Min Risk: A score of 100 indicates that all questions were answered correctly and the risk for that third party would be Min Risk (Minor).<br>**Note:** Each organization in a particular risk domain inherits the scoring method and weight of the risk area definition. Third-party risk managers can override the values when needed. |
| Default weight | The default weight for third parties in this risk domain. |




### What to do next

Continue with the checklist of required setup procedures.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create and configure an external questionnaire

As part of any due-diligence process, you send multiple questionnaires and possibly document requests to the third-party contact. To simplify this ongoing task, you define questionnaire templates and document-request templates and then group them into reusable assessment templates.

## Before you begin

Roles required: admin or sn_vdr_risk_asmt.vendor_risk_admin for questionnaire and document request templates and sn_vdr_risk_asmt.vendor_risk_manager for assessment templates.

## About this task

As part of an assessment, the TPR manager can send multiple questionnaires and document requests by using assessment templates. The TPR admin first defines the required questionnaire templates and document request templates and then the TPR managers groups them into an assessment template. The TPR manager can use the resulting assessment template to send the appropriate questionnaires, document requests, or both in future assessments.

Send an external risk assessment to a third party to collect the data that you use to determine their risk. An assessment during the early stages of the procurement process helps you to select the best qualified third party from a pool of candidates.

For example, you can generate an assessment template for critical third parties that requires both SOC1 and SOC2 reports and a different assessment template for medium-risk third parties that requires only SOC1. In both cases, you can use the existing SOC1 document request template.

As an ongoing process, you also send assessments to existing third parties to update their risk level.

### Terminology in TPRM

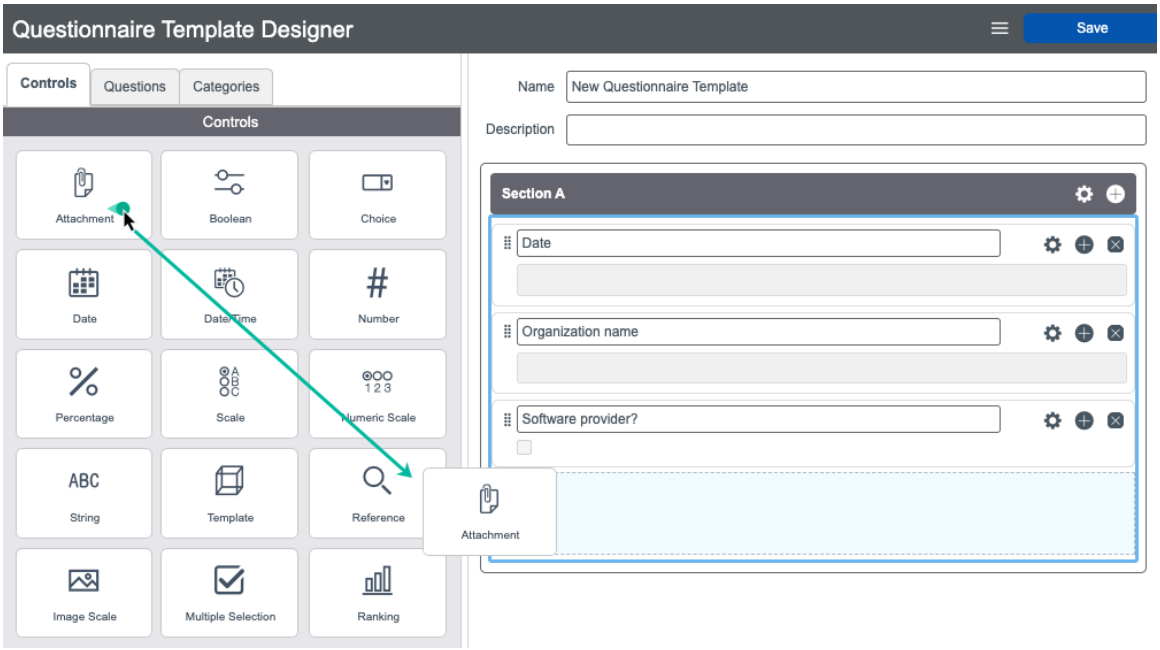
| Term | Description |
|---|---|
| Metric or Assessment metric | A single question within a questionnaire template. |
| Metric type or Assessment metric type | A questionnaire template. |
| Category or Assessment category | A set of related questions within a questionnaire template.<br><br>**Note:** There can be multiple categories within a metric type. |

## Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Assessment Setup** > **Questionnaire Templates** and then select **New (Designer)**.
2. Drag controls onto the form, apply categories, and optionally assign correct responses to each question.

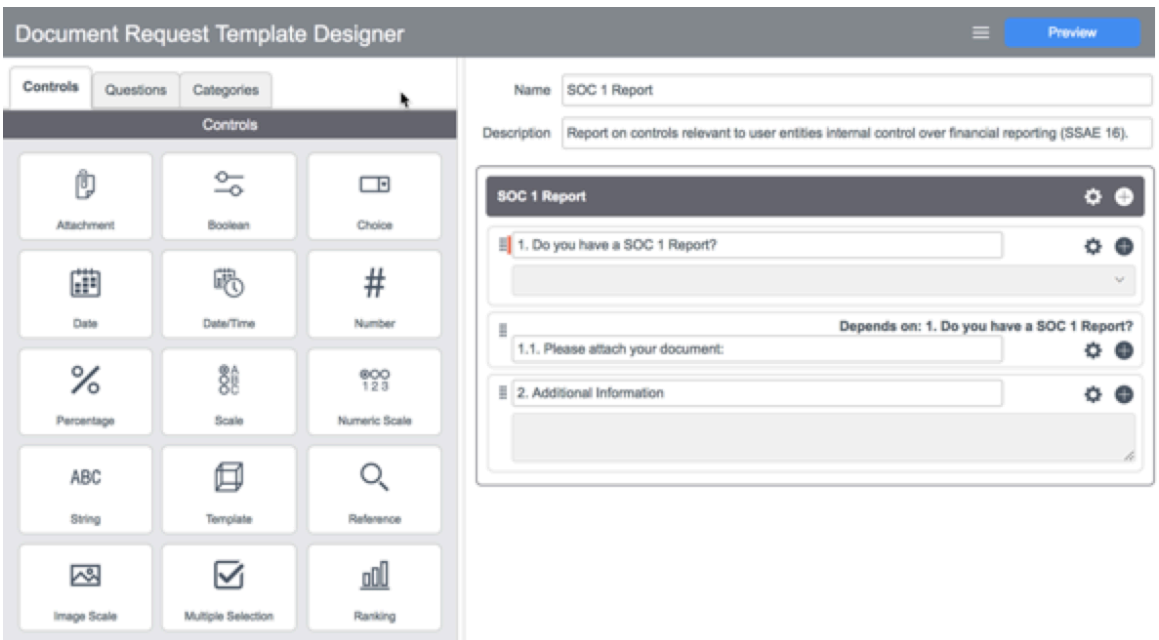
   For further detail, you can also navigate to the platform view to modify things such as weights at both the category and question level.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. Navigate to **Third-party Risk Management** > **Assessment Setup** > **Document Request Templates** and select **New (Designer)**.
4. Drag controls onto the form to create an assessment that specifically requests evidence or documentation.

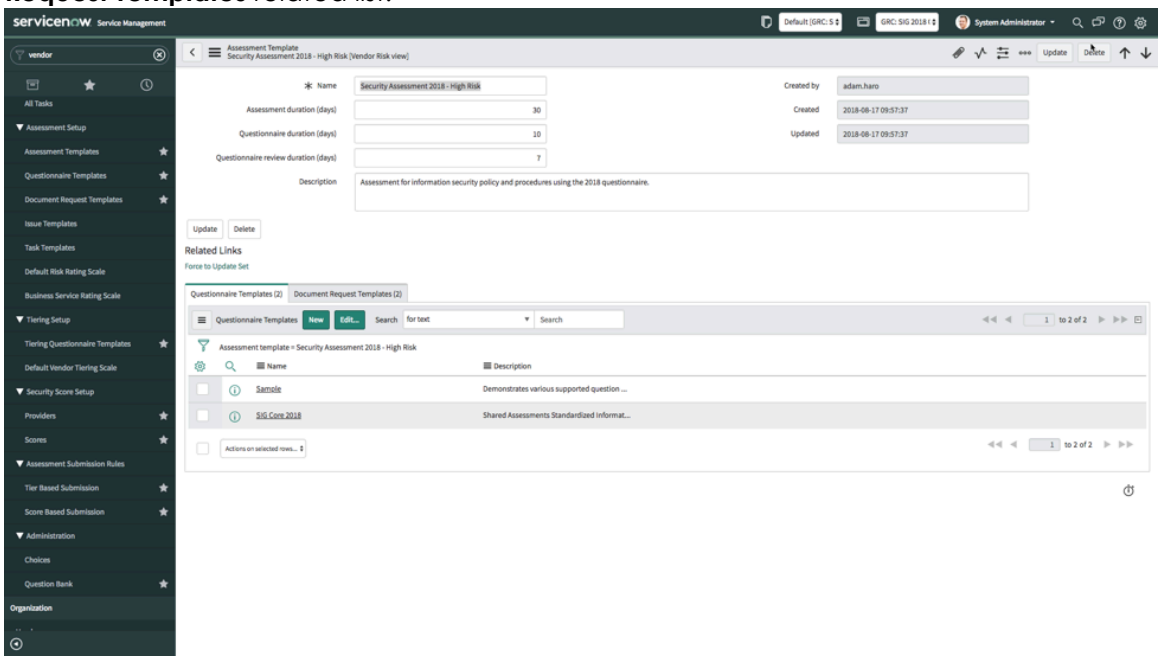
   This example is a request for SOC1 evidence.




5. Navigate to **Third-party Risk Management** > **Assessment Setup** > **External Assessment Templates** and select **New**.
6. Fill in the required fields and select **Submit**.
7. Navigate back to the newly created Assessment Template and under the **Questionnaire Templates** related list, select **Edit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Add the required Questionnaire Templates and repeat the same steps for the **Document Request Templates** related list.




### Set up and maintain a question bank

After you add a question to a question bank, you can reuse it in any assessment by dropping it into the assessment. You can create custom questions, add existing questions, or add and customize the sample questions that are included with the base system.

#### Before you begin

Role required: admin or sn_vdr_risk_asmt.vendor_risk_admin

#### Procedure

1. Define an assessment category.
   Navigate to **All** > **Third-party Risk Management** > **Administration** > **Question Bank**, and then select **New**.
2. Enter a descriptive name and description for the assessment category and then save the record.
3. Add an assessment metric (a question) to the category using one of the following methods:
   - Create a question as described in Define a question.
   - Add a question from an existing questionnaire or questionnaire template.
4. Select **Update** to save the questions to the question bank in the current assessment category.

### Define a question

After you add a question to a question bank, you can reuse it in any assessment by dropping it into the assessment. You can create custom questions, add existing questions, or add and customize the sample questions that are included with the base system.

#### Before you begin

Role required: admin or sn_vdr_risk_asmt.vendor_risk_manager

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## About this task

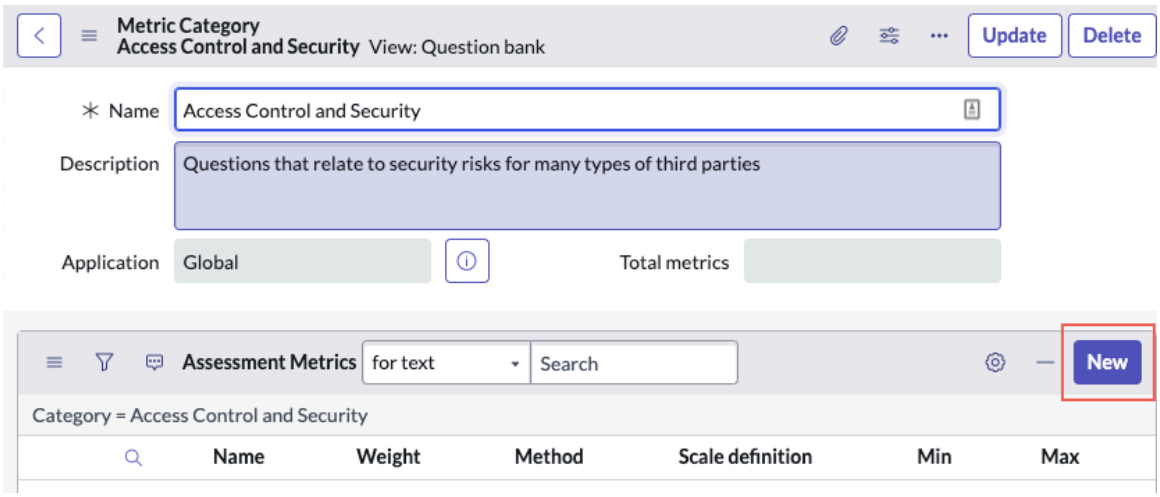
### Terminology in TPRM

| Term | Description |
|---|---|
| Metric or Assessment metric | A single question within a questionnaire template. |
| Metric type or Assessment metric type | A questionnaire template. |
| Category or Assessment category | A set of related questions within a questionnaire template.<br><br>**Note:** There can be multiple categories within a metric type. |

## Procedure

1. Define or select the assessment category that is appropriate for the question that you plan to add.
   - To select an existing assessment category, navigate to **All** > **Third-party Risk Management** > **Administration** > **Question Bank**, and then select it in the list.
   - For instructions on defining an assessment category, see Set up and maintain a question bank.
2. Create an assessment metric (a question).

   In the **Assessment Metrics** related list for the assessment category, select **New** and then fill in the form.




### Assessment Metric form

| Field | Description |
|---|---|
| Name | A name for the assessment metric. |
| Mandatory | Indicates whether the question must be answered. |
| Weight | A numerical value used to compare the importance of this metric to other metrics. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Category | The category to which the metric is associated. |
| Question | The question to be displayed on the questionnaire. |
| Description | Tooltip text to help the third-party contact better understand the question. |
| Details | An expanded description for the question that is displayed to the assessment taker. The details can include text, images, video, and links to external websites or other content.<br>**Note:** You can define the details at the assessment level or at the category level. |

3. Select the **General** tab and then fill in the values.

**Assessment Metric form — General tab**

| Field | Description |
|---|---|
| Method | The method used for gathering data for the metric.<br>◦ Assessment<br>◦ Default answer from field<br>◦ Default answer from script<br>◦ Script |
| Order | Order that the question will be displayed in the questionnaire. Questions with lower values for **Order** appear earlier in the questionnaire. |
| Active | Activates the metric for assessments and results calculations. |
| Depends on | The identifier for a separate metric (question). The answer to the question that is specified in this field determines whether the question that you're currently defining is displayed to the user.<br>The field appears only if you select **Assessment** in the **Method** field. |
| Default answer | The field from which the default answer for the question comes.<br>This field appears only if you select **Default answer from field** in the **Method** field. |
| Ask question | Specifies whether the question requires an answer when a default value is provided.<br>The field appears only if you select **Default answer from field** or **Default answer from script** in the **Method** field. |
| Script | The scripts used to produce performance indicators for the associated metric when the assessment is generated.<br>The field appears only if you select **Default answer from script**or **Script** in the **Method** field. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** To enter a tab character in your script, use the **Tab** key. For tab actions, press **Esc** to tab forward and **Shift+Esc** to tab backward. |

4. Select the **Question Type** tab and then fill in the form.

**Note:** The fields that appear depend on the **Data type** that you select.

**Assessment Metric form — Question Type tab**

| Data type | Description and additional fields |
|---|---|
| Attachment | On questionnaires, users attach one or more files to a question. |
| Check box | On questionnaires, users select a check box for a statement or leave it cleared.<br><br>To define a single metric to be scored for the data type, select **Scored** and select a **Correct answer** for the question.<br><br>If you didn't select the **Scored** check box, set the **Scale definition**. If a selected check box equates to a good score, set the field to **High**. If a small numerical value should be interpreted as a positive score, set the field to **Low**. |
| Choice | On questionnaires, users select a value from a list of custom answer options. Create a metric definition for each answer option.<br><br>Select the **Randomize answers** check box to randomize the order of answer options for a question.<br><br>Select the **Reference table** to use for reference data type questions.<br><br>Define conditions to restrict choices to those that meet the selection criteria.<br><br>To define a single metric to be scored for the data type, select **Scored** and then select a correct answer for the question.<br><br>If you didn't select the **Scored** check box, set the **Scale definition** value.<br>◦ If a selected check box is a good score, set to **High**.<br>◦ If a small numerical value is a good score, set to **Low**.<br><br>You can select the **Maximum Normalization input** check box to calculate assessment scores for questions using a normalization input value. For more information, see Normalize the scores for metrics. |
| Date | On questionnaires, users select a date. |
| Date/Time | On questionnaires, users select a date and time. |
| Duration | On questionnaires, users specify an answer that falls within the **Min**/**Max** range.<br><br>Select the **Dependent plugin** that the duration depends upon: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Data type | Description and additional fields |
| --- | --- |
| | ◦ Asset Management<br>◦ CMDB<br>◦ Core<br>◦ Cost Management<br>◦ Procurement<br>◦ Software Asset Management<br><br>To define a single metric to be scored for the data type, select **Scored** and select a **Correct answer** for the question.<br><br>If you didn't select the **Scored** check box, set the **Scale definition**.<br>◦ If a large numerical value is a good score, set the field to **High**.<br>◦ If a small numerical value is a positive score, set the field to **Low**. |
| Image Scale | On questionnaires, users select an image scale.<br><br>To define a single metric to be scored for the data type, select **Scored** and select a **Correct answer** for the question. You must unlock the **Correct answer** field to make changes.<br><br>If you didn't select the **Scored** check box, set the **Scale definition**.<br>◦ If a large numerical value is a good score, set to **High**.<br>◦ If a small numerical value is a good score, set to **Low**. |
| Likert Scale | On questionnaires, users select a value from a custom scale of answer options. Create a metric definition for each answer option, which is represented by a selection button on the scale. A Likert scale metric that evaluates an application's ease of use might have **Easy**, **Average**, and **Difficult** metric definitions.<br><br>Select **Randomize answers** to randomize the order of answer options for the question.<br><br>To define a single metric to be scored for the data type, select **Scored** and select a **Correct answer** for the question. You must unlock the **Correct answer** field to make changes.<br><br>If you didn't select the **Scored** check box, set the **Scale definition**.<br>◦ If a large numerical value is a good score, set to **High**.<br>◦ If a small numerical value is a good score, set to **Low**. |
| Multiple Selection | On questionnaires, users select one or more values from a list of custom answer options. For the **Multiple Selection** data type, you have the option to specify a **Reference table** and conditions that filter, which values from the table are displayed in the list.<br><br>For example, if you select **Country [core_country]** as the reference table and set the conditions as **Name** + **starts with** + **B**, the query returns only the 19 countries that start with the letter B, instead of the full list of 231 countries. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Data type | Description and additional fields |
| --- | --- |
| | To define a single metric to be scored for this data type, select **Scored** and select a **Correct answer** for the question. You must unlock the **Correct answer** field to make changes.<br><br>If you didn't select the **Scored** check box, set the **Scale definition**.<br>◦ If a large numerical value is a good score, set to **High**.<br>◦ If a small numerical value is a good score, set to **Low**.<br><br>You can select the **Maximum Normalization input** check box to calculate assessment scores for questions using a normalization input value. For more information, see Normalize the scores for metrics. |
| Number | On questionnaires, users enter a number that falls within the **Min**/**Max** range.<br><br>To define a single metric to be scored for this data type, select **Scored** and select a **Correct answer** for the question.<br><br>If you didn't select the **Scored** check box, set the **Scale definition**.<br>◦ If a large numerical value is a good score, set to **High**.<br>◦ If a small numerical value is a good score, set to **Low**. |
| Numeric Scale | On questionnaires, users enter a number that falls within the **Min**/**Max** range.<br><br>To define a single metric to be scored for this data type, select **Scored** and select a **Correct answer** for the question.<br><br>If you didn't select the **Scored** check box, set the **Scale definition**.<br>◦ If a large numerical value is a good score, set to **High**.<br>◦ If a small numerical value is a good score, set to **Low**. |
| Percentage | On questionnaires, users enter a percentage number that falls within the **Min**/**Max** range.<br><br>To define a single metric to be scored for this data type, select **Scored** and select a **Correct answer** for the question.<br><br>If you didn't select the **Scored** check box, set the **Scale definition**.<br>◦ If a large numerical value is a good score, set to **High**.<br>◦ If a small numerical value is a good score, set to **Low**. |
| Ranking | On questionnaires, users can select a different order number for each option to rank them. A user can either fill in the number or drag an option.<br><br>Select **Randomize answers** to randomize the order of answer options for the question.<br><br>Set the **Scale definition**.<br>◦ If a large numerical value equates to a good score, set the field to **High**.<br>◦ If a small numerical value should be interpreted as a positive score, set the field to **Low**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Data type | Description and additional fields |
|---|---|
| Reference | On questionnaires, users select a value from a list that is generated from a specified **Reference table**. For example, a user could select a user name in response to a question if you specify User [sys_user] as the reference table.<br><br>You also have the option of defining conditions for limiting the information pulled from the reference table into manageable chunks. |
| String | On questionnaires, users enter text. The size of the string field depends on the **String option** you select:<br>◦ Single line<br>◦ Single line wide<br>◦ Multiline |
| Template | On questionnaires, users select a value from a predefined series of answer options. There must be at least one template defined to use this data type. For a template, there's a template definition for each answer option, which is represented by a radio button.<br><br>To define a single metric to be scored for this data type, select **Scored** and select a **Correct answer** for the question. You must unlock the **Correct answer** field to make changes.<br><br>If you didn't select the **Scored** check box, set the **Scale definition**.<br>◦ If a large numerical value is a good score, set to **High**.<br>◦ If a small numerical value is a good score, set to **Low**. |
| Yes/No | On questionnaires, users select **Yes** or **No** from a list.<br><br>To define a single metric to be scored for this data type, select **Scored** and select a **Correct answer** for the question.<br><br>If you didn't select the **Scored** check box, set the **Scale definition**.<br>◦ If a **Yes** answer is a good score, set to **High**.<br>◦ If a **No** answer is a good score, set to **Low**. |

5. Select **Update** to save the questions to the question bank.

### View the sample questions in the base system

TPRM includes sample questionnaires that you can use to define questionnaire templates for your organization.

#### Before you begin

To include sample questionnaires, you select **Load demo data** while installing TPRM. See Configuring Third-party Risk Management for installation instructions.

Role required: admin or sn_vdr_risk_asmt.vendor_risk_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

- Sample questions don't include scoring or right/wrong answers — you define those attributes.
- Sample questions aren't updated to support regulatory changes — you manage changes.

### Procedure

Navigate to **All** > **Third-party Risk Management** > **Assessment Setup** > **Questionnaire Templates**.

**Terminology in TPRM**

| Term | Description |
|---|---|
| Metric or Assessment metric | A single question within a questionnaire template. |
| Metric type or Assessment metric type | A questionnaire template. |
| Category or Assessment category | A set of related questions within a questionnaire template.<br>**Note:** There can be multiple categories within a metric type. |

The Assessment Metric Types list displays the list of metric types. Each metric type includes one or more metric categories. Each metric category includes multiple sample questions.

Related topics

Using the SIG questionnaire for risk assessment

#### Normalize the scores for metrics

You can use the **Maximum normalization input** setting to use normalized values to calculate assessment scores for questions (metrics).

## When 'Maximum normalization input' applies

The **Maximum normalization input** field appears only when:

- The data type of the question is either **Choice** or **Multiple Selection**.
- The **Scored** check box is not selected.

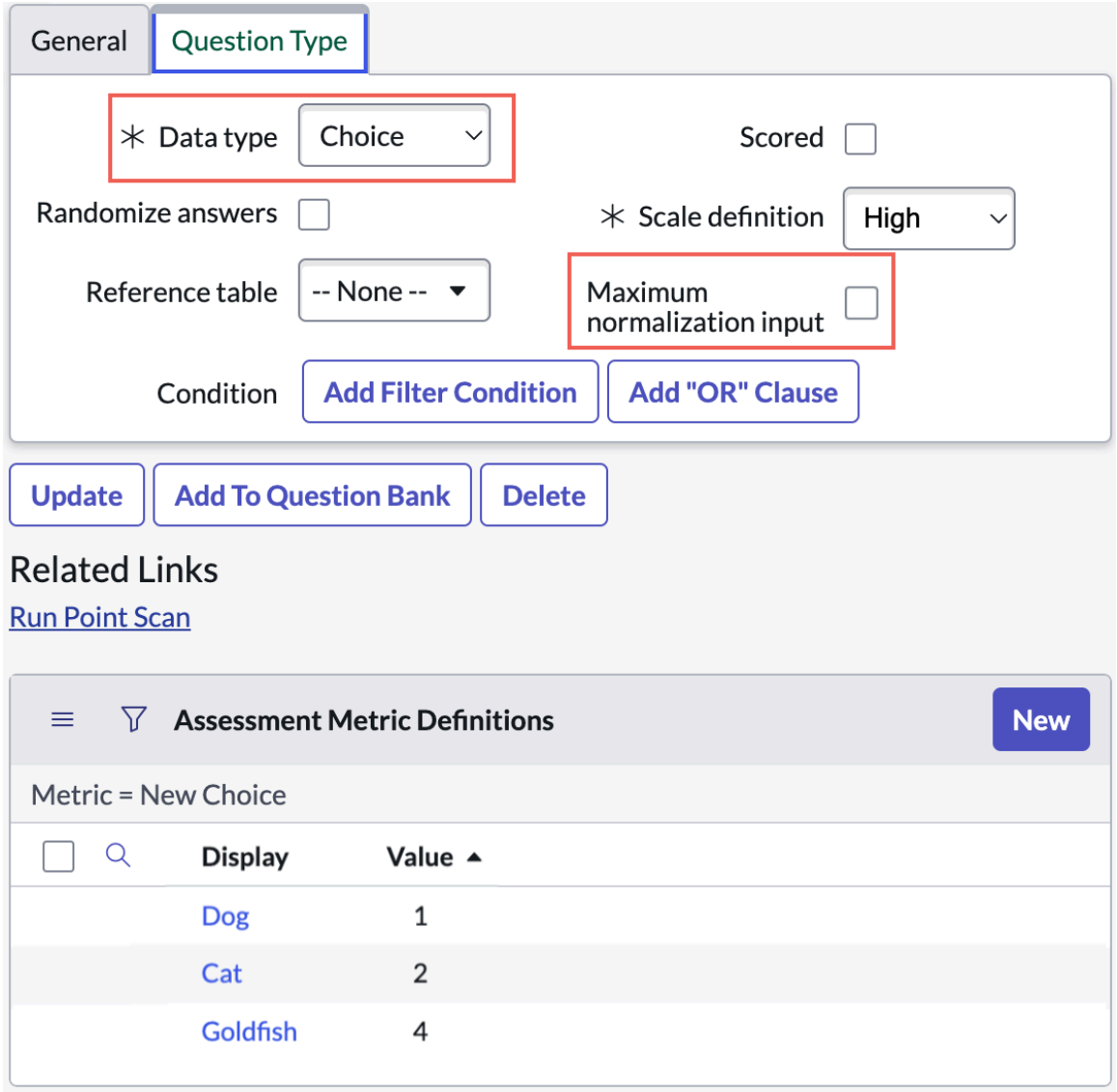
To use normalized scoring, the value assigned to each metric definition (possible answer) for each metric (question) must be unique.

In the following examples, the **Scale definition** is **High** (larger numerical values are good).

## 'Choice' type questions

When 'Maximum normalization input' is not selected

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




Formula: ( [Value of the response] – [Lowest value] ) / ( [Highest value] – [Lowest value] ) * 100.

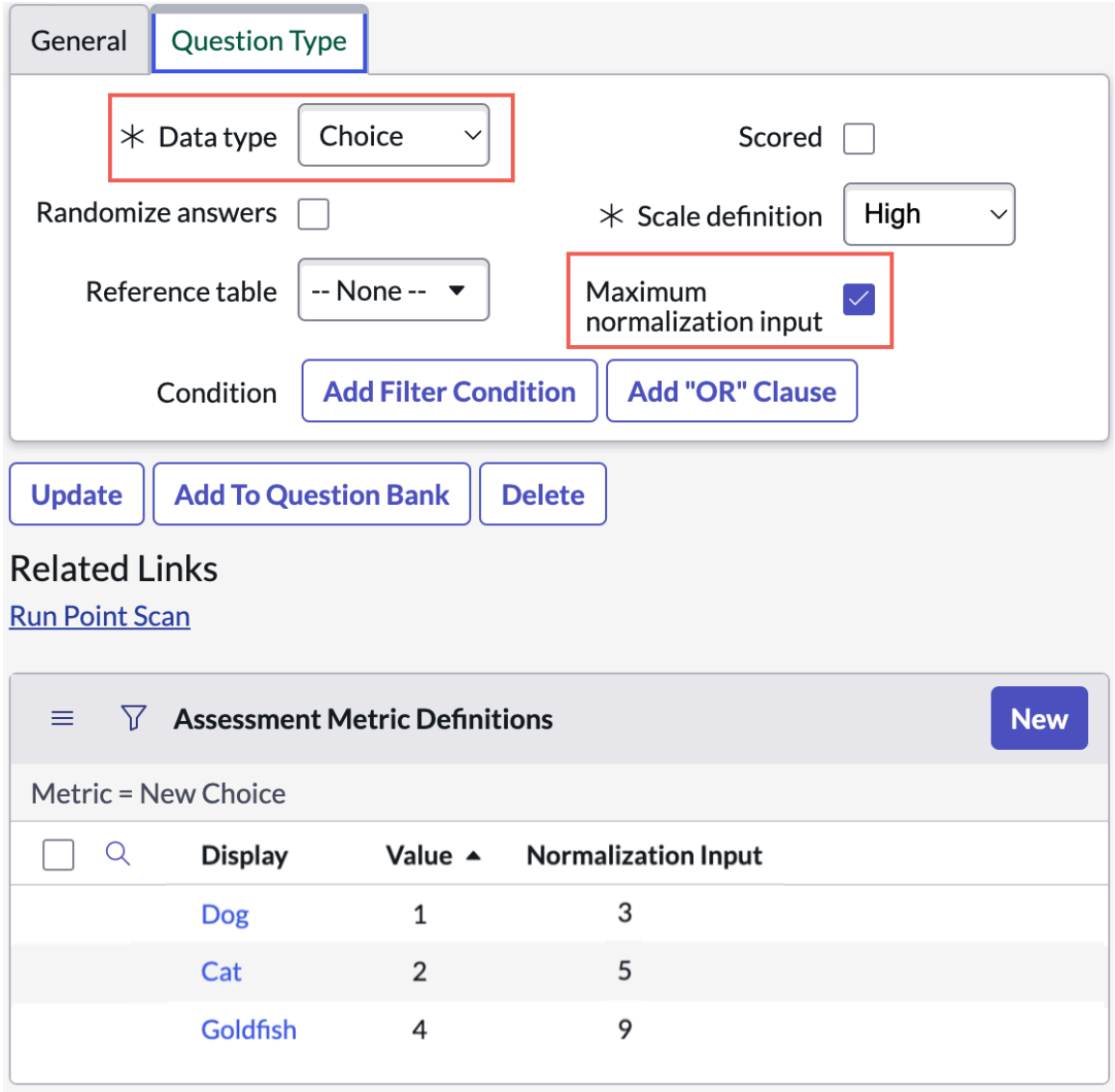
In this example, the question allows a choice among answers with values of `1`, `2`, and `4`.

**Scores**

| Response | Calculation | Score |
|---|---|---|
| Dog | [(1-1)/(4-1)] * 100 | 0 |
| Cat | [(2-1)/(4-1)] * 100 | 33 |
| Goldfish | [(4-1)/(4-1)] * 100 | 100 |

When 'Maximum normalization input' is selected

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




Formula: `( [Value of the response]/ [Highest value] ) * 100`.

In this example, the question allows a choice among answers with values of `1`, `2`, and `4` and normalization input values of `3`, `5`, and `9` respectively.

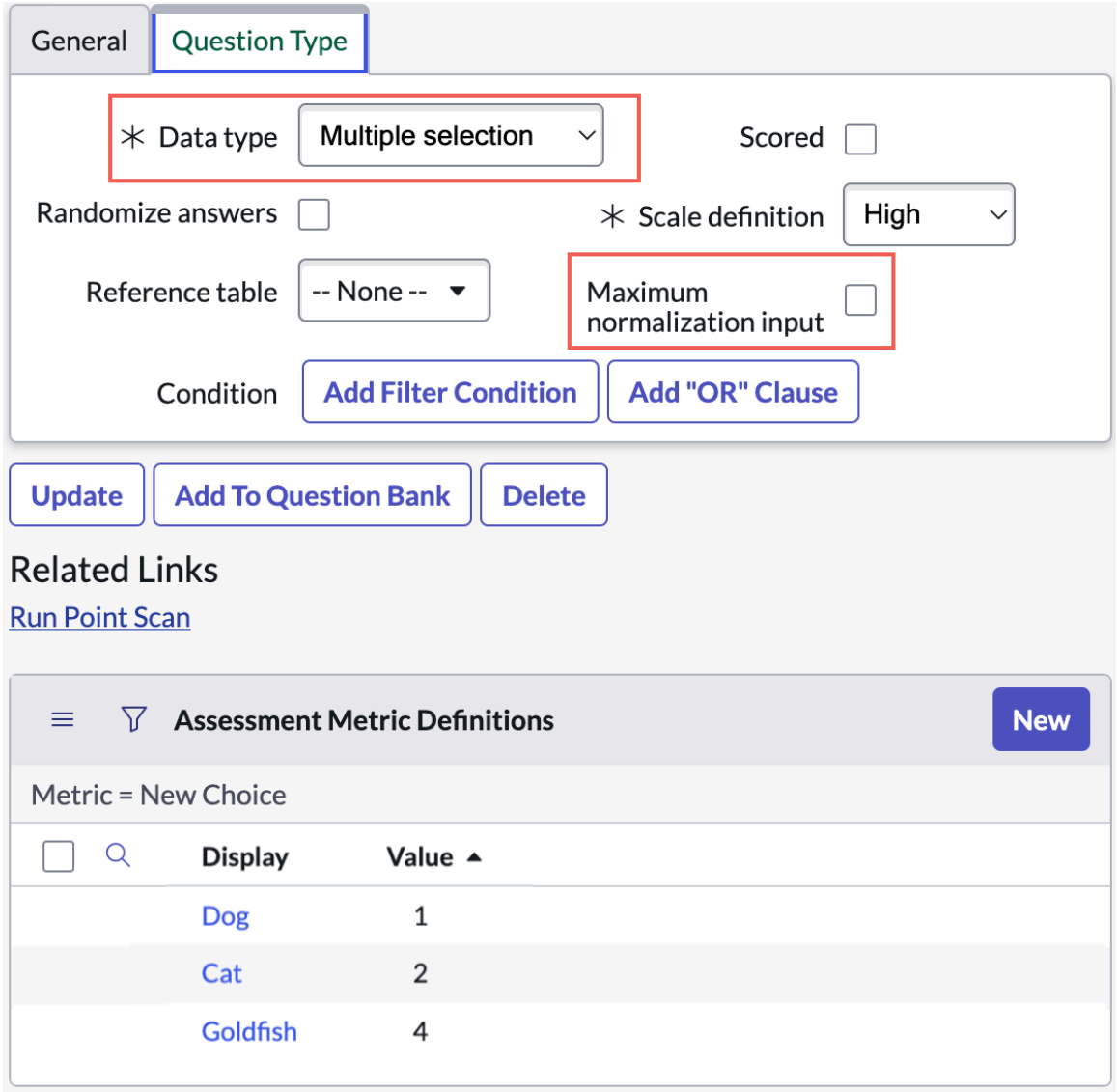
**Scores**

| Response | Calculation | Score |
|---|---|---|
| Dog | (1 / 4) * 100 | 25 |
| Cat | (2 / 4) * 100 | 50 |
| Goldfish | (4 / 4) * 100 | 100 |

### 'Multiple selection' type questions

When 'Maximum normalization input' is not selected

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




Formula: `( [Sum of the selected values]/ [Sum of the Normalization input values] ) * 100`.

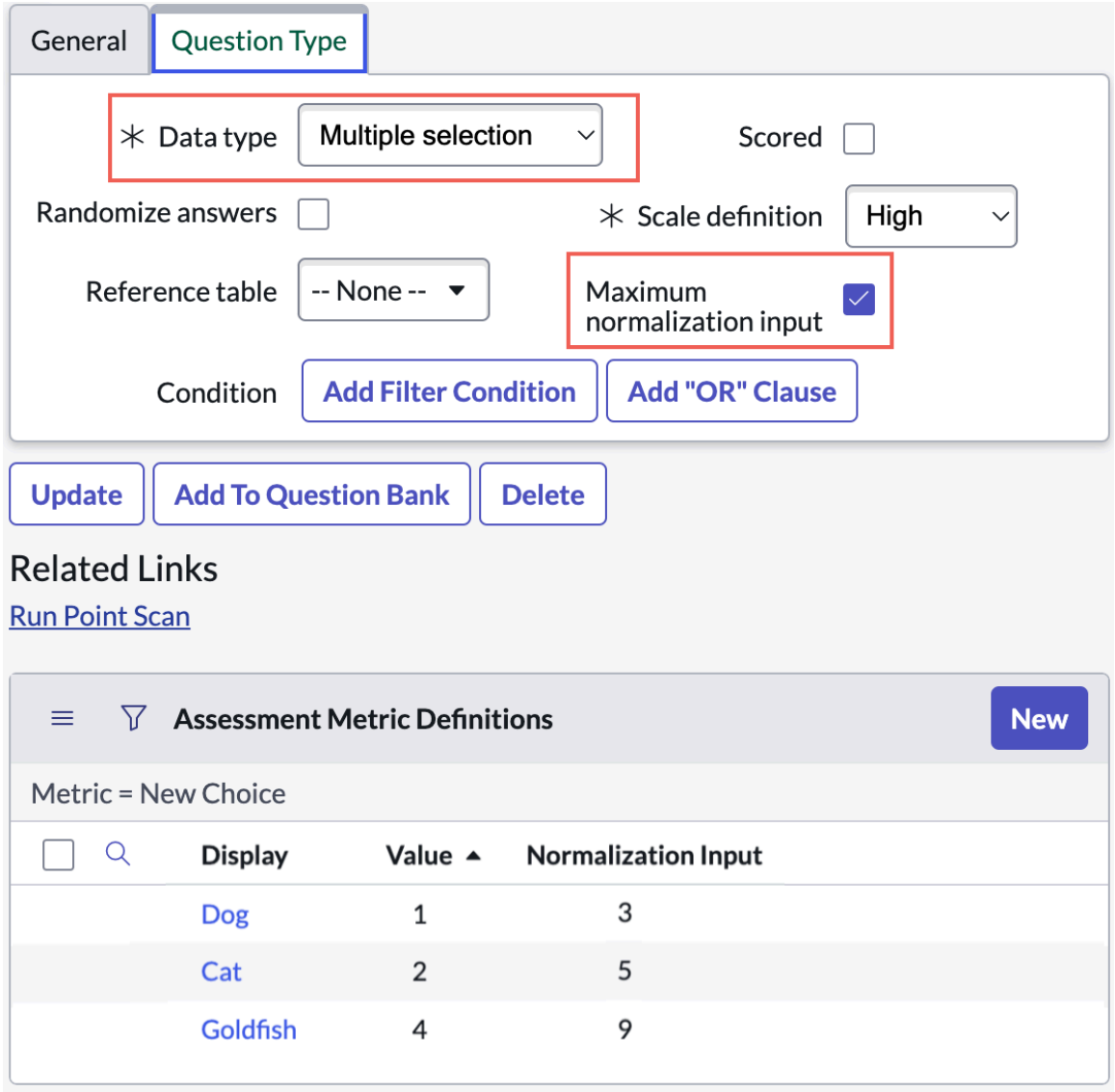
In this example, the question allows a multiple selections among answers with values of `1`, `2`, and `4`.

**Scores**

| Response | Calculation | Score |
|---|---|---|
| Dog and Cat | ([1+2] / 17) * 100 | 47 |
| Cat | (2 / 17) * 100 | 11.8 |
| Cat and Goldfish | ([2+4] / 17) * 100 | 50 |
| Goldfish | (4 / 17) * 100 | 100 |

When 'Maximum normalization input' is selected

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




- The system uses the value `0` for the response that has the lowest value. In this example, the **Dog** response is assigned the value `0`.
- Formula for each selection: ( `[Normalization input value for the response]/ [Maximum of the Normalization input values] ) * 100`.
- The score for the metric (question) is the maximum calculated score among all responses.

In this example, the user selects **Dog** and **Cat**.

- The score for the **Dog** response is `(0 / 9) * 100 = 0`.
- The score for the **Cat** response is `(5 / 9) * 100 = 55.5`.
- The score for the overall metric is `55.5`.

Formula: `( [Sum of the selected values]/ [Sum of the Normalization input values] ) * 100`.

In this example, the question allows a multiple selections among answers with values of `1`, `2`, and `4`.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Scores

| Response | Calculation | Score |
|---|---|---|
| Dog and Cat | ([1+2] / 17) * 100 | 47 |
| Cat | (2 / 17) * 100 | 11.8 |
| Cat and Goldfish | ([2+4] / 17) * 100 | 50 |
| Goldfish | (4 / 17) * 100 | 100 |

## Create an assessment template

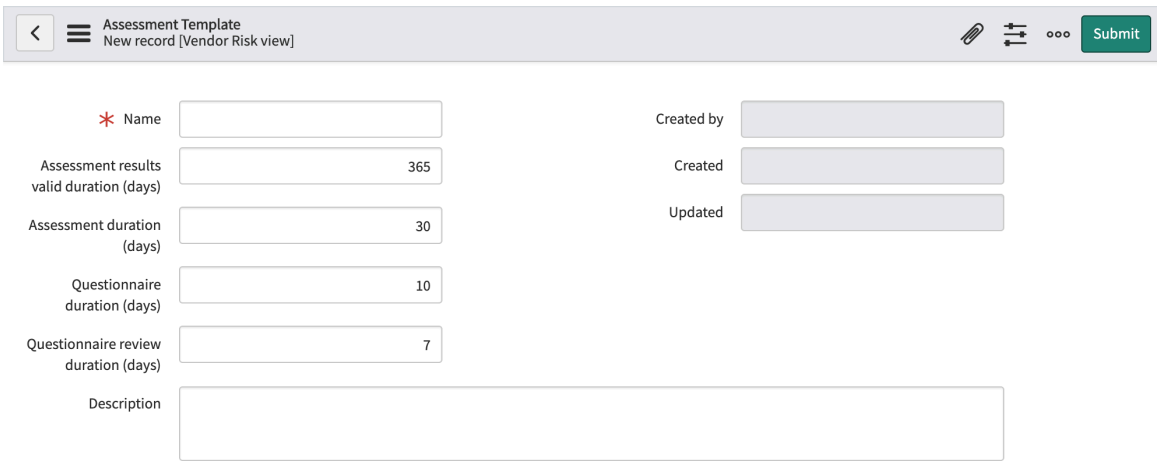
When defining an assessment template, the third-party risk manager provides scheduling information for the third-party risk assessment.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager

### Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Assessment Setup** > **External Assessment Templates**.
2. Select **New**.




3. On the form, fill in the fields.

### Assessment Templates form

| Field | Description |
|---|---|
| Name | Name of the assessment template. |
| Assessment results valid duration (days) | The number of days that the default assessment will be valid. |
| Assessment duration (days) | Time provided for the entire external risk assessment to be completed. |
| Questionnaire duration (days) | Time allocated for the assessor to complete the questionnaire portion of the assessment. |
| Questionnaire review duration (days) | Time allocated for the third-party risk admin to review the responses provided to questionnaire. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Created by | User who created the template. |
| Created | Time when the template was created. |
| Updated | Time when the template was last updated. |
| Description | Description of the assessment. |

4. Select **Submit**.

### Result
Any other templates associated with this assessment template are shown as related links or tabs.

## Create a questionnaire template or document request template

You can reuse questionnaire templates and document-request templates to speed up the creation of new questionnaires and document requests.

### Before you begin
Role required: admin or sn_vdr_risk_asmt.vendor_risk_admin

### About this task
When defining a template, you specify whether questionnaires or document requests should require electronic signatures for the third party and/or the reviewer as mandated by your organization's rules or federal regulations.

### Procedure
1. Navigate to **All** > **Third-party Risk Management** > **Assessment Setup** > **Questionnaire Templates** or **Third-party Risk Management** > **Assessment Setup** > **Document Request Templates**.
2. Select **New**, fill in the fields, and then select **Submit**.
   The Assessment Metric Type form opens.

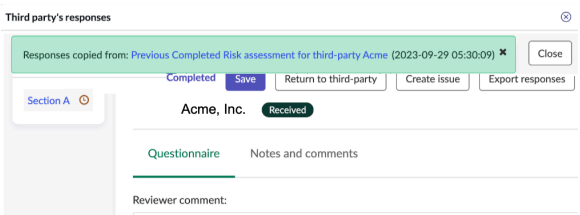
#### Terminology in TPRM

| Term | Description |
|---|---|
| Metric or Assessment metric | A single question within a questionnaire template. |
| Metric type or Assessment metric type | A questionnaire template. |
| Category or Assessment category | A set of related questions within a questionnaire template.<br>**Note:** There can be multiple categories within a metric type. |

#### Assessment Metric Type form

| Field | Description |
|---|---|
| Name | The name of the template. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Vendor risk area | Select the third-party risk domain that applies to the type of third party that will receive the questionnaire or document request. For example, if you select the Security risk domain, then only third parties that are assigned that risk domain will receive the questionnaire or document request.<br><br>For more information, see Define a third-party risk domain. |
| Third-party signature required | Option to require the third party's primary contact to provide an electronic signature in the Third-party portal.<br><br>**Note:** You can use electronic signatures to certify that the third-party contact has successfully reviewed and approved the questionnaire responses or document request. |
| Reviewer signature required | Option to require the reviewer to review the validity of the assessment responses and provide an electronic signature as final approval. |
| Description | A description for the template. |
| Include previous responses | Option to pre-populate the questionnaire with responses from a completed questionnaire (status is **Complete**) in a previous closed assessment. The TPR admin [sn_vdr_risk_asmt.vendor_risk_admin] role is required.<br><br>**Important:** While editing a questionnaire, you can override the option that is specified in the questionnaire template.<br><br>The entry in the Third-party portal notifies the third-party contact that responses were copied. As shown in the example, the notification includes a link to the assessment that supplied the responses and its closing date.<br><br>  <br><br><br>◦ The responses are populated when the new questionnaire is submitted to the third-party contact.<br>◦ The source questionnaire must be based on the same template as the current questionnaire.<br>◦ If multiple source questionnaires are available, then the questionnaire from the most recent closed assessment is used.<br>◦ For engagements, only questionnaires that were used in engagements are used.<br>◦ For third-party onboarding, only questionnaires that were used in third-party onboardings are used.<br>◦ Attachments aren't copied. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ Answers of type **Duration**, **Date**, and **Date/Time** aren't copied.<br>◦ The setting can't be changed after the questionnaire is sent to the third party.<br><br>To specify the maximum age for source questionnaires, configure the **Maximum age for reusing responses** `sn_vdr_risk_asmt.max_age_for_questionnaire_reuse` system property. See Configure TPRM properties. |

Any other templates associated with this template are shown as related links or tabs.

Related topics

Create an external risk assessment — Legacy process

### Create a document request template

Use the Document Request Template designer to create and edit questionnaire templates that you can use as the basis for other templates.

#### Before you begin

Role required: admin or sn_vdr_risk_asmt.vendor_risk_admin

**Note:** Three default questions are created for each new document request template.

#### Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Assessment Setup** > **Document Request Templates**.
2. Select **New (Designer)**.

**Tabs on the designer**

| Tab | Description |
|---|---|
| Controls | Supported question data types are available in the Controls palette. Drag a control onto the designer canvas to create a question of that type. |
| Questions | A library of questions for various categories, so you don't have to build each questionnaire from scratch. |
| Categories | Assessment open in the **Design** view. The questionnaire **Name** field appears above the first category in the canvas. A empty question field appears in the category container. |

3. Enter a name and then drag a control onto the designer canvas to create a question of that type.

**Note:** For each metric that will be scored, specify the correct answer. Scored metrics determine the compliance status of the risk.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Question controls

| Data type | Description | Scored |
|---|---|---|
| Attachment | Question with a Manage Attachments icon for users to attach one or more files. | Y |
| Boolean | Question with a check box or a **Yes/No** list for user responses. | N |
| Choice | List of predefined options. For more information, see the definition for **Choices**. | Y |
| Date | Date field. | N |
| Date/Time | Date and time field. | N |
| Number | Number field with predefined minimum and maximum values. The default is 1–10. | N |
| Percentage | Percentage field with a prescribed range. | N |
| Scale | Predefined Likert scale. Answer options appear as radio buttons. | Y |
| Numeric Scale | Selectable number scale. The default is 1–5. Answer options appear as radio buttons. | Y |
| String | Single or multi-line text field. | N |
| Template | Choice list of templates that provide a predefined scale of options. | Y |
| Reference | Choice list of fields from a specified reference table. This data type doesn't support reference qualifiers. | N |
| Image Scale | Choice list of images you can use for scales. | N |
| Multiple Selection | List of selectable choices. Multiple choices are allowed. | N |
| Ranking | Selectable scale for ranking choices. | N |

4. Select the menu icon to select one of the following options:

**Note:** The availability of each option depends on the status of the open questionnaire.

| Option | Description |
|---|---|
| Save | Save the current document request. |
| Preview | Display a preview of the document request. |
| New Document Request | Open a fresh canvas for a document request. |
| Open Document Request | Open a list of existing document requests that you can select and edit. |
| Copy Document Request | Copy the document request and edit. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create a questionnaire template using the Designer

Use the Questionnaire Template Designer to create and edit questionnaire templates that you can use as the basis for other templates.

## Before you begin

Role required: admin or sn_vdr_risk_asmt.vendor_risk_admin

#### Terminology in TPRM

| Term | Description |
|---|---|
| Metric or Assessment metric | A single question within a questionnaire template. |
| Metric type or Assessment metric type | A questionnaire template. |
| Category or Assessment category | A set of related questions within a questionnaire template.<br><br>**Note:** There can be multiple categories within a metric type. |

**Note:** A questionnaire template must have at least one category. Each category must contain at least one question.

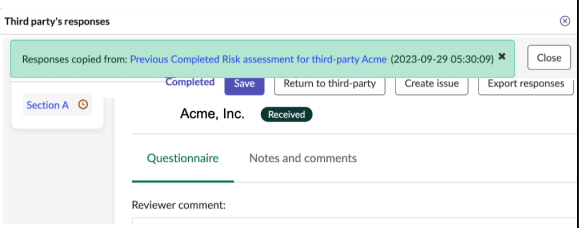
## Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Assessment Setup** > **Questionnaire Templates**.
2. Select **New** and then fill in the form.

#### Assessment metric type form

| Field | Description |
|---|---|
| Name | |
| Third-party risk area | Select the third-party risk domain that applies to the type of third party that will receive the questionnaire or document request. For example, if you select the Security risk domain, then only third parties that are assigned that risk domain will receive the questionnaire or document request.<br><br>For more information, see Define a third-party risk domain. |
| Classification | Select **Questionnaire template**. |
| State | Value that the system auto-assigns. |
| Description | Text that describes the questionnaire to help other users to understand its intent. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Third-party signature required | Option to require that the third-party contact digitally signs the questionnaire before submitting it. |
| Reviewer signature required | Option to require that one of the assessors digitally signs the questionnaire before the request for due diligence can be approved. |
| Include previous responses | Option to pre-populate the questionnaire with responses from a completed questionnaire (status is **Complete**) in a previous closed assessment. The TPR admin [sn_vdr_risk_asmt.vendor_risk_admin] role is required.<br><br>**Important:** While editing a questionnaire, you can override the option that is specified in the questionnaire template.<br><br>The entry in the Third-party portal notifies the third-party contact that responses were copied. As shown in the example, the notification includes a link to the assessment that supplied the responses and its closing date.<br><br>  <br><br>◦ The responses are populated when the new questionnaire is submitted to the third-party contact.<br>◦ The source questionnaire must be based on the same template as the current questionnaire.<br>◦ If multiple source questionnaires are available, then the questionnaire from the most recent closed assessment is used.<br>◦ For engagements, only questionnaires that were used in engagements are used.<br>◦ For third-party onboarding, only questionnaires that were used in third-party onboardings are used.<br>◦ Attachments aren't copied. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Answers of type **Duration**, **Date**, and **Date/Time** aren't copied.<br>◦ The setting can't be changed after the questionnaire is sent to the third party.<br><br>To specify the maximum age for source questionnaires, configure the **Maximum age for reusing responses** `sn_vdr_risk_asmt.max_age_for_questionnaire_reuse` system property. See Configure TPRM properties. |

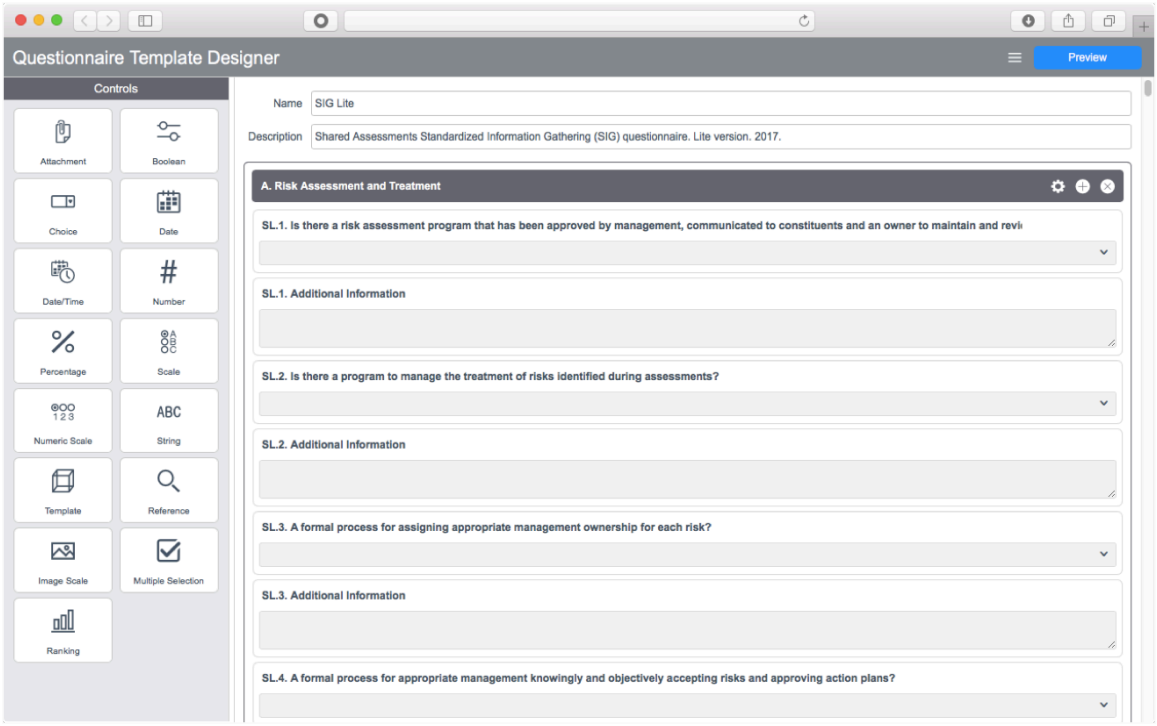
3. Right-click in the form header and select **Save**.
   The system generates two related lists and adds the **Edit in Designer** link.
4. Select the **Edit in Designer** link.
5. Select the menu icon to select one of the following options:

   **Note:** The availability of each option depends on the status of the open questionnaire.

| Option | Description |
| --- | --- |
| Save | Save the current questionnaire. |
| Preview | Display a preview of the questionnaire with its current settings. |
| New Questionnaire | Open a fresh canvas for a new questionnaire. |
| Open Questionnaire | Open the list of existing questionnaires. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
| --- | --- |
| Copy Questionnaire | Create a copy of the questionnaire that you can edit. |




### Import a questionnaire from a spreadsheet

If you maintain questionnaires using Microsoft Excel spreadsheets, you can save time and effort by importing your spreadsheet data directly into TPRM tables. You can then create questionnaires automatically from templates.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager

### About this task

Before you import questionnaires, you must validate that the data in the spreadsheet meets certain requirements. To assist you before you import the spreadsheet, you can review the formatting requirements and view or download a sample spreadsheet to use as a guide. See Guidelines for importing spreadsheet data.

You can specify the following property settings:

Text delimiter in spreadsheets [`sn_vdr_risk_asmt.excel_choice_delimiter`]

Character string that separates response text in questions of type 'Choice' and 'Multiple Selection'.

Common delimiters: \r, \n, \t, \r\n, and the comma character.

Maximum spreadsheet file size [`sn_vdr_risk_asmt.excel_file_max_size`]

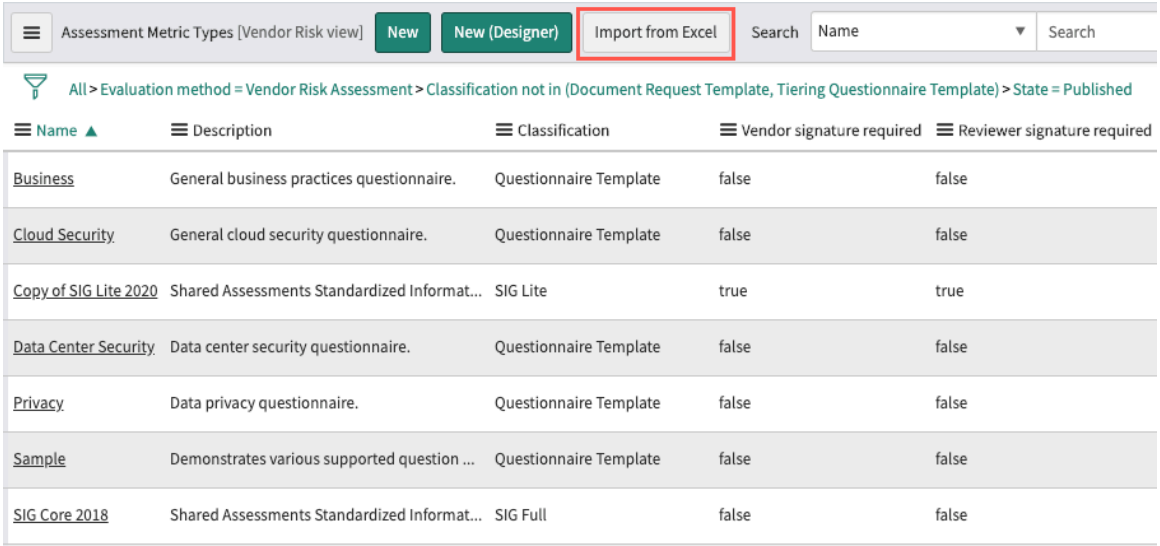
Maximum file size in MB that can be imported.

See Configure TPRM properties.

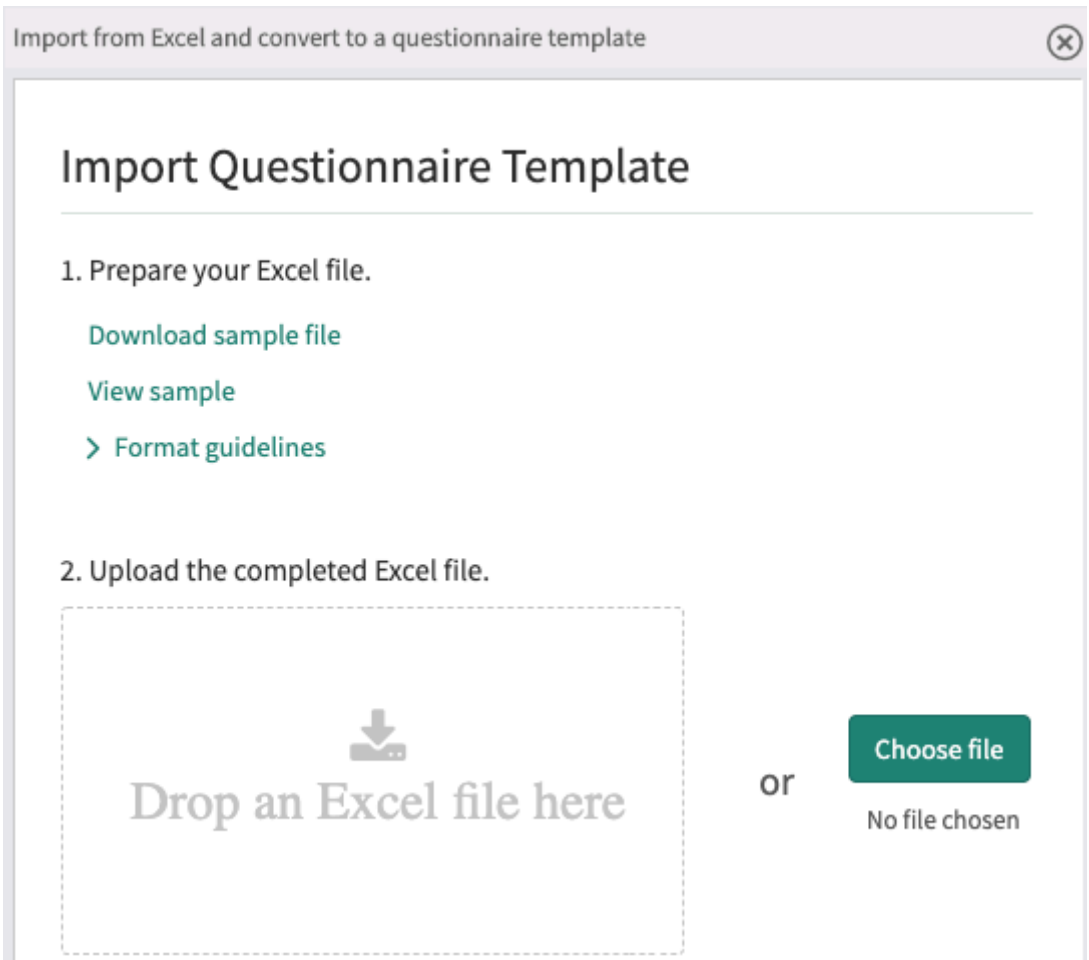
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Assessment Setup** > **Questionnaire Templates** or to **Third-party Risk Management** > **Tiering Setup** > **Tiering Questionnaire Templates**.
2. Click **Import from Excel** to open the Import Questionnaire Template form.




| Name ▲ | Description | Classification | Vendor signature required | Reviewer signature required |
|---|---|---|---|---|
| Business | General business practices questionnaire. | Questionnaire Template | false | false |
| Cloud Security | General cloud security questionnaire. | Questionnaire Template | false | false |
| Copy of SIG Lite 2020 | Shared Assessments Standardized Informat... | SIG Lite | true | true |
| Data Center Security | Data center security questionnaire. | Questionnaire Template | false | false |
| Privacy | Data privacy questionnaire. | Questionnaire Template | false | false |
| Sample | Demonstrates various supported question ... | Questionnaire Template | false | false |
| SIG Core 2018 | Shared Assessments Standardized Informat... | SIG Full | false | false |



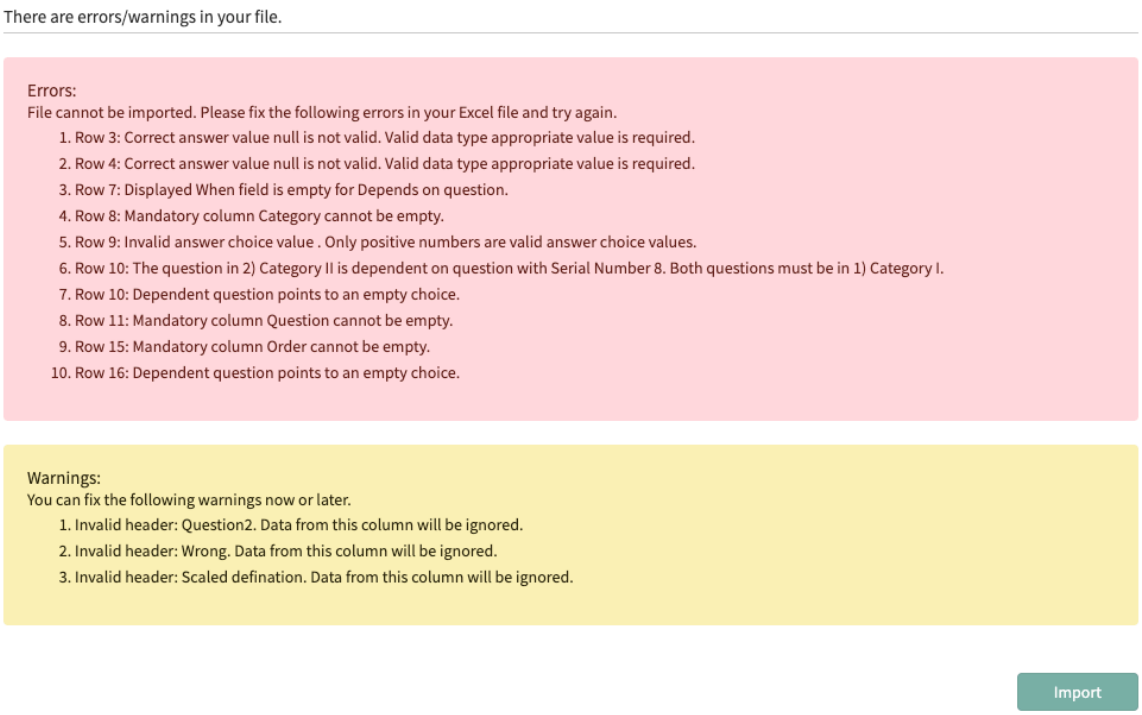

3. Perform any or all of the steps in the **Prepare your Excel file** section:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Click **Download sample file** to download an active worksheet that is properly formatted for import into Third-party Risk Management. You can use the sample as a guide for reformatting your own spreadsheet, or you can copy data from your spreadsheet directly into the sample.
- Click **View sample** to open an image of a properly-formatted worksheet. You can compare this with your existing worksheet to validate that it contains the same columns and question formats.
- Click **Format guidelines** to view Guidelines for importing spreadsheet data.

4. When your spreadsheet is ready for import, either drag it into the **Drop an Excel file here** box, or click **Choose File**, navigate to your Excel file, and then click **Open**.

   Errors and warning appear if the file is formatted incorrectly. You must fix all errors before the questionnaires can be imported. You can import a file that has only warnings, but there might be issues in the resulting question data.



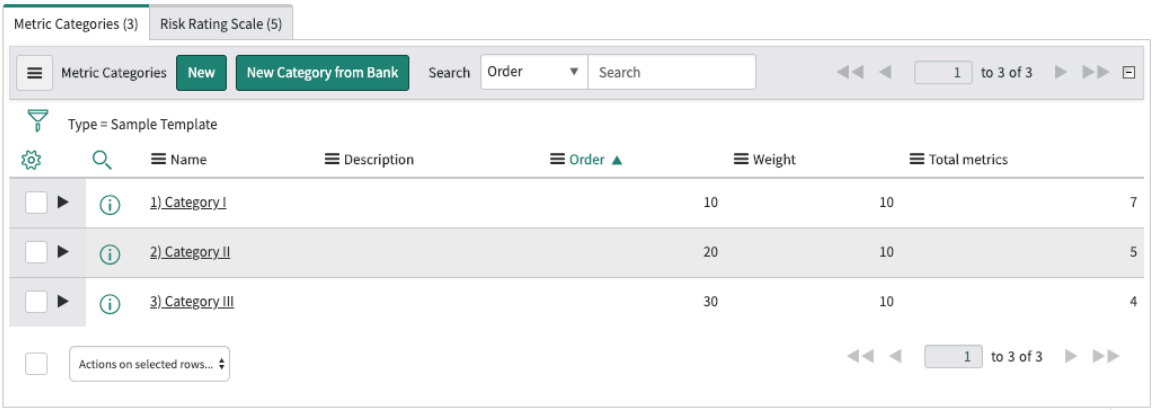

> **Note:** If there are warnings, you can continue with the import, but issues might arise. Consider fixing all errors and warnings before you import questionnaires.

5. After you have fixed errors and warnings, enter a name for the template, and then click **Import**.

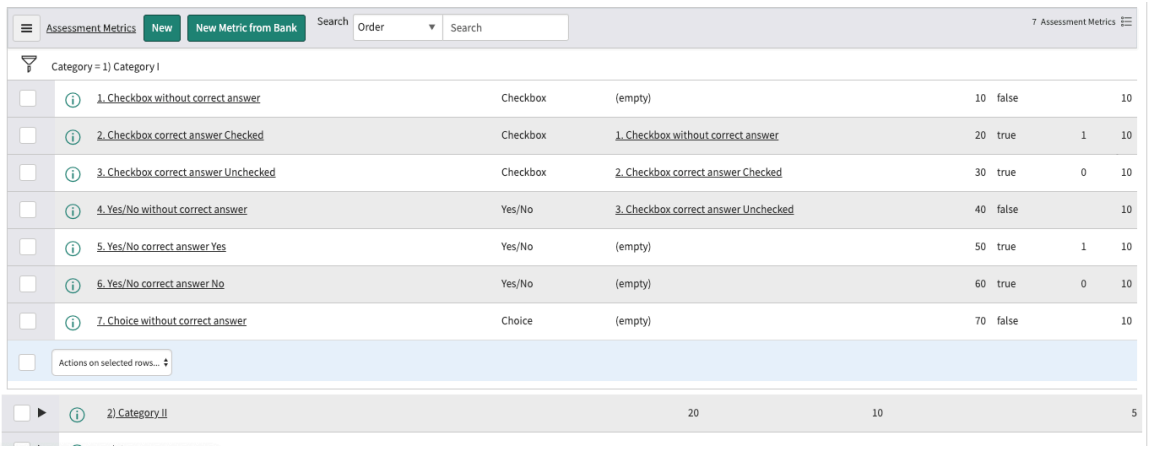
   The name must be unique. The name defaults to the worksheet name in your spreadsheet.

   A confirmation pop-up displays the imported questionnaire.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




6. You can expand a category to view the questions in each category.




Related topics

- Guidelines for importing spreadsheet data
- Import existing data from other systems

### Set up the approval levels for due diligence requests

Assign one or more approval levels to the users or groups that approve your due diligence requests in the Third-party Risk Management application. Because the approval levels are applied iteratively and each level contains different rules, you can help to ensure that the correct user or group is assigned as an approver.

#### Before you begin

Role required: admin or sn_vdr_risk_asmt.vendor_risk_admin

#### About this task

You can create up to 10 different approval levels that each contain different approval rules. Within each approval level, you can assign one or more rules with different filter conditions that apply to the assigned approvers. For example, you might want different approvers to be assigned to the due diligence request depending on the engagement's risk rating and location.

With the Third-party due diligence default configuration, you can create three records with approval levels 1, 2, and 3. Level 1 has three rules, level 2 has two rules, and level 3 has two rules. The following example shows how you would assign these rules with filter conditions:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Level 1
  - Rule 1: User A and User B are assigned to approve the engagement's low risk rating.
  - Rule 2: User C and User D are assigned to approve the engagement's medium risk rating.
  - Rule 3: User E and User F are assigned to approve the engagement's high-risk rating.
- Level 2
  - Rule 1: Third-party risk (TPR) manager is assigned to approve the engagement in Asia/Pacific.
  - Rule 2: TPR manager is assigned to approve the engagement in Europe/North America.
- Level 3
  - Rule 1: All TPR administrators are assigned to approve an engagement in a specific region that has a high-risk rating.
  - Rule 2: All TPR administrators are assigned to approve an engagement in a specific region that has a very high-risk rating.

During the approval process, level 1 is triggered first. If all assigned users approve the conditions in level 1, then level 2 is triggered and so on. If any assigned user in level 1 has rejected the due diligence request, level 2 isn't triggered and the due diligence request is rejected. For more information on possible rating definitions, see Set up risk rating scales and scoring.

**Note:** You can use the Third-party due diligence default configuration included as part of the base system or deactivate the default configuration and create an approval configuration that applies to a different table. For more information, see Set up approval configuration.

### Procedure

1. Navigate to **All** > **Approval Configurator** > **Approval Configurations**.
2. Select **Third-party due diligence default configuration**.
3. Create an approval level by selecting **New**.
   A **Third-party due diligence default level** is included as part of the base system.
4. On the form, fill in the fields.

**Approval Level form**

| Field | Description |
|---|---|
| Name | Name for the approval level. |
| Level | Stage of approval. |

**Note:** In an approval configuration, you can't have multiple approval levels with the same level number. The rules of each level are applied sequentially, one after the other.

5. Select **Submit**.

Related topics

Set up the approval rules for due diligence requests

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Set up the approval rules for due diligence requests

Set up the rules at each approval level for your due diligence requests by selecting an approver type and the number of approvals that you require in the Third-party Risk Management application. You can also filter the table conditions that apply to each rule so that you can help ensure that the correct user or group is assigned as an approver.

## Before you begin

Set up the approval levels. For more information, see Set up the approval levels for due diligence requests.

Role required: admin or sn_vdr_risk_asmt.vendor_risk_admin

## About this task

For each rule, you can select the individual approvers, approvers from the Third-party due diligence request [sn_tprm_dd_request] table, or dynamic approvers. The approvers can be a Third-party risk (TPR) manager or TPR administrator.

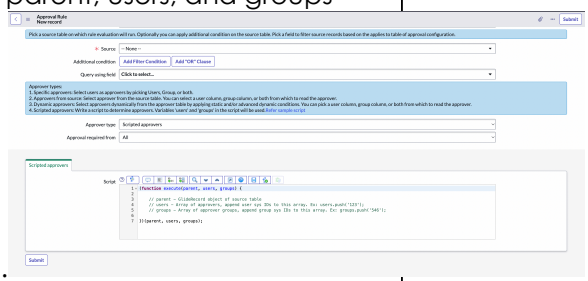
## Procedure

1. Navigate to **All** > **Approval Configurator** > **Approval Configurations**.
2. Select an approval configuration record.
3. In the Name column of the Approval Levels section, select the approval level record that you want.
4. In the Approval Rules section, select **New**.
5. On the form, fill in the fields.

**Approval Rule form**

| Field | Description |
|---|---|
| Name | Name of the approval rule. |
| Source | Table to which the approval rule is applied.<br><br>Third-party due diligence request [sn_tprm_dd_request] table is the source table for due diligence requests. |
| Query using field | Field that connects the approving table and the source table.<br><br>**Note:** This field is only required if you're not using the Third-party due diligence request [sn_tprm_dd_request] table as a source. |
| Additional condition | Filter conditions that you can apply on the source table.<br><br>These filter conditions determine when the rule is applied. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Approver type | Type of approver:<br>◦ Specific approvers: Your choice of approvers.<br>◦ Approver from source: Users or groups from the source table.<br>◦ Dynamic approvers: Approvers that are selected dynamically from any table.<br>◦ Scripted approvers: Script to determine your approvers. In the following example, a new approval rule record is shown with Scripted approvers as the selected **Approver type**. A script is started where you can update the parent, users, and groups parameters.<br>  <br>**Note:**<br>For security reasons, a user with the admin role doesn't have write access to the **Script** field on the Approval Rule form. Only the Approver Configurator developer has create and write access to the **Script** field on the Approval Rule form.<br>If you have the admin role, you can set up an approval rule only with the following types of approvers from the Approver type list:<br>◦ Specific approvers<br>◦ Approver from source<br>For more information on the roles in the GRC: Approver Configurator application, see Roles installed with GRC: Approver Configurator. |
| Approval required from | Any user or all stakeholders from whom the approval is required. |
| Description | Brief note that describes the approval rule. |
| Approvers | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Approvers from | Approver table.<br><br>This field is available only if the Approver type is **Approver from source** or **Dynamic approvers**. This field defaults to the source table if the approver is from the source table. |
| Filter by | Conditions to filter records from the approver table.<br><br>This field is available only if the Approver type is **Dynamic approvers**. |
| Advanced | Option to set a scripted dynamic condition. |
| User field | User reference or list of approvers from the approver table. |
| Group field | User group reference as approver from the approver table. |
| Dynamic condition | Script field to apply an advanced filter on the approver table. |
| Users | One or more users that are designated as approvers. |
| Group | Group of approvers. |
| Scripted approvers | |
| Script | Script to determine approvers. **users** and **groups** in the script are selected as approvers. |

6. Select **Submit**.

Related topics

Set up the approval levels for due diligence requests

## Requesting third-party risk due diligence

Request third-party risk due diligence to determine the level of risk for interactions with a third party, engagement, or fourth party by using Third-party Risk Management. You conduct due diligence to become aware of the associated risks so that you can make informed decisions, establish appropriate controls, and mitigate the potential negative impact when working with external parties.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Any employee at your organization can request due diligence, which is an investigation or examination of business relationship risk, for an engagement.

- An engagement is the informal or contracted relationship that you intend to form with a third party that could potentially expose your organization to risk. The engagement outlines the services or products to be provided by the third party and other details of the relationship.
- A third party is any organization or individual that you've interacted or entered into a business relationship with. Third parties can have subsidiaries and can contract with fourth parties. For example, departments are subsidiaries.
- A fourth party can contract with further parties. All downstream parties, such as the fourth through the nth parties, carry risk in the same ways as third parties.

A Third-party risk (TPR) manager reviews the request for due diligence for the engagement and approves it. If the information provided by the requester was insufficient or the engagement isn't possible for your organization, the TPR manager rejects it. The IRQ process starts after the TPR approver [sn_vdr_risk_asmt.approver] or TPR manager approves it. For more information, see Due diligence workflow and Assessing your third-party risk.

For more information about the terms that are used in these sections or why you might conduct due diligence, see Terminology and Why you conduct due diligence

To learn more about creating a due diligence request, see Request due diligence for a third-party engagement. When creating a due diligence request, the following options are available:

- **Onboard a new engagement** Start the onboarding process for a new engagement with an existing third party. For more information about this type of onboarding, see Example — Onboarding a third party.
- **Reassess an existing engagement** Reassess an existing engagement when the conditions change. For example, let's say that you hear adverse news or have changes in your third-party's supply lines. You might want to reassess the risk by conducting additional due diligence.
- **Reassess an existing engagement for contract renewal** Reassess the risk before your organization renews the contract with a current third party or engagement by conducting due diligence.
- **Offboard an engagement with due diligence** Determine if offboarding (terminating the relationship) with an engagement is the optimal course of action by conducting due diligence. For example, it might be too risky to switch third parties or engagements even if their current performance doesn't meet expectations.

  Extenuating circumstances can contribute to the decision. For example, if the third party is sourcing materials that are difficult to obtain, switching providers might be costly and introduce additional risks. In such cases, continuing with the existing third party, with whom a long-term relationship exists, might be preferable to mitigate potential disruptions and higher risks.

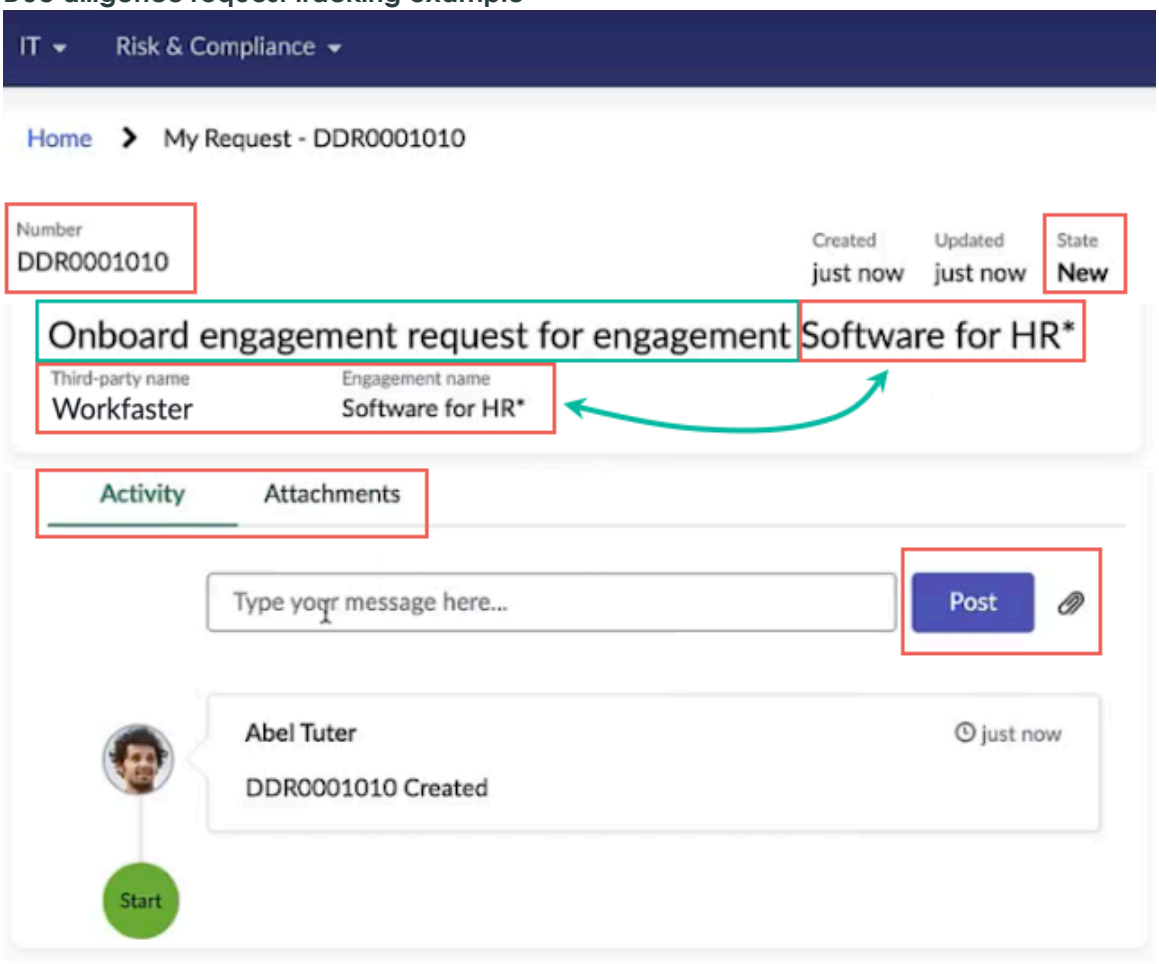
- **Offboard an engagement with no due diligence** Request that an engagement be permanently terminated when an engagement ends or you want to switch to a different third party for other reasons. In this case, you typically don't need to conduct additional due diligence. The process does, however, include the normal Inherent Risk Questionnaire (IRQ) process to confirm that the services provided by the engagement will no longer continue. For more information about this type of offboarding, see Offboarding an engagement without conducting due diligence.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

For each due diligence request, the system auto-assigns a unique ID number that starts with the text **DDR**. Use the ID to track your request. You can post a message to reviewers and add attachments from the page.

The following example shows how a new due diligence request appears.

**Due diligence request tracking example**




## Request due diligence for a third-party engagement

Request due diligence to assess the risk that is associated with doing business with an engagement. By conducting due diligence, you gain access to the most up-to-date, comprehensive, and accurate information before making a decision on entering into a business relationship.

### Before you begin

Role required: snc_internal

### About this task

Because your organization assesses the risk that is associated with doing business with third parties, it performs due diligence for any engagement with a third party. When you request due diligence, you specify the third party's name and the reason for your request. For example, start a new engagement with a third party that you have already engaged or perform due diligence in preparation to renew a contract. You then specify the details that help the Third-party Risk (TPR) managers and TPR assessors at your organization proceed with the due diligence processes. If a request is accepted, it initially goes through the IRQ process. After the IRQ process, as part of the Due diligence process, two third-party risk assessments begin. One assessment is for the third party and another assessment is for the engagement. For more information, see Due diligence workflow.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** This feature is available only if the Third-party Risk Management application has been activated. After you install the Risk concentration map feature, you must install a Google license to enable the feature. To enable the risk concentration map feature, see Enable the TPRM Risk concentration map.

### Procedure

1. Navigate to **All** > **Self-Service** > **Employee Center** to open your Employee Center and then select **Risk & Compliance**.
2. Select the **Request due diligence for third-party risk** card.
3. On the request form, specify the purpose of your request.
   - **Onboard a new engagement**
   - **Reassess an existing engagement**
   - **Reassess an existing engagement for contract renewal**
   - **Offboard an engagement with due diligence**
   - **Offboard an engagement with no due diligence**

     For more information, see Offboarding an engagement without conducting due diligence.

   For descriptions of each type of due diligence request, see Requesting third-party risk due diligence.
4. Optional: Select **Add attachments** to include a document with the request.
5. Specify the third party for the engagement.

   You can request due diligence either for an engagement with a third party that you're already engaged with or for an engagement with a new third party.

   **Note:** You can reactivate a third party that is in the **Terminated** status. Terminated third parties appear in the list for requests of the **Onboard a new engagement** type. If such a request is accepted and closed, the third party's status is changed to **Active**.

   - For an engagement with an existing third party or with a department, partner, subsidiary, or fourth party of the third party:
     a. Select the third party from the list.
     b. The form expands and the system auto-populates the key information for the third party including the address and contact details.
     c. In the next step, enter the key information like the address and contact details for the engagement.
   - For a new third party:
     a. Select the **Third party is not listed** check box.
     b. Enter the name of the new third party.
     c. The form expands. In the next step, you enter the key information like the address and contact details for the third party and for the engagement.
6. Fill in the fields and then select **Submit**.
   If you selected an existing third party, much of the information is automatically filled in. For descriptions of these fields, see Request third-party risk due diligence request form.
7. Select **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The system opens to the **Activity** tab on the My request page. For each due diligence request, the system auto-assigns a unique ID number that starts with the text **DDR**. Use the ID to track your request. You can post a message to reviewers and add attachments from the page.
- The system sends you an email confirmation that your request was submitted. The message includes a link to the request details on the Third-party Risk Management application.
- The system sends an email notification to all users in the group that is specified in the **Assignment group**. The message states that the request was received and is in the **New** state. The message also includes a link to the details page for the request.

**Note:** For new due diligence requests, the **Assignment group** is set to Due diligence request assigners. The TPR manager or owner can specify which group is the **Assignment group** on the **Details** tab for a due diligence request. For more information, see Due diligence request process management and Add users to groups based on responsibilities.

Related topics

Offboarding an engagement without conducting due diligence

### Offboarding an engagement without conducting due diligence

Request that an engagement be permanently terminated when an engagement ends or you want to switch to a different third party for other reasons. In this case, you typically don't need to conduct additional due diligence. The process does, however, include the normal Inherent Risk Questionnaire (IRQ) process to confirm that the services provided by the engagement will no longer continue.

The user who is assigned as **IRQ assessor** is responsible for completing the questionnaire specifying why the engagement is no longer required. After the IRQ is completed, the approval process formally offboards the engagement and sets it to the inactive state.

When the engagement is set as inactive, future auto-scheduled due diligence or information requests aren't sent to the engagement contacts.

## Assessing your third-party risk

Use Third-party Risk Management to identify and assess potential risks that are associated with your third-party relationships. The information gathered from internal questionnaires, external questionnaires, and documentation requests helps you to understand the third party's risk profile, determine the appropriate risk mitigation strategies, and determine whether the third party or engagement meets all necessary compliance requirements.

### Responding to questionnaires

The following processes outline the timing and methods for responding to internal and external questionnaires:

Inherent Risk Questionnaire (IRQ) process

After the due diligence request is approved by the Third-party risk (TPR) manager [sn_vdr_risk_asmt.vendor_risk_manager], the IRQ assessor [snc_internal] completes the internal risk assessment by responding to the IRQ.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After the IRQ assessor submits their responses and the TPR manager or owner reviews and closes the IRQ, the due diligence request state updates from IRQ in progress to IRQ in review.

Based on the information gathered, the TPR manager and their team assess the potential risks that are associated with the engagement. They evaluate factors such as the financial stability, the operational capacity, the adherence to quality standards, the compliance with regulations, and the third party's ability to meet delivery timelines. This assessment helps the team to understand the third party's risk profile and to determine the appropriate risk mitigation strategies.

For more information about IRQs, see Respond to an Inherent Risk Questionnaire (IRQ).

Due diligence process: Compliance verification

When the IRQ process is completed, the TPRM application sends questionnaires and requests for documentation to the third party and engagement. As part of an assessment, your organization might send multiple questionnaires and document requests. For example, the TPR manager might request the third party's certifications, licenses, or audit reports to validate compliance.

**Note:** The TPR manager can develop assessment templates to simplify and automate the process of determining which questionnaires and document requests to send to a third party of this type. The TPR administrator can define questionnaire templates, document request templates, and then the TPR manager can group them into an assessment template. Your organization can reuse the template to send the questionnaires and document requests to similar third parties in future assessments. For more information about the templates, see Create a questionnaire template or document request template and Create a document request template.

The TPR manager and their team use the third party's responses and internal analysis to determine whether the third party meets all the necessary compliance requirements. These requirements could include verifying the third party's compliance with applicable laws and regulations, such as environmental regulations, labor laws, and anti-corruption policies.

Due to the sensitive nature of the items involved, the TPR manager and their team evaluate the third party's data security and privacy practices. They assess the third party's information security measures, data protection policies, access controls, and vulnerability management processes. If the third party has access to proprietary information or customer data, they might require the third party to undergo a cybersecurity audit or provide evidence of their data protection measures.

For more information about reviewing responses, see Review responses to external questionnaires.

**Note:** Your TPR assessor can export received or returned questionnaires to Microsoft Excel spreadsheets. This option enables your organization to use the spreadsheet environment to review the questions and answers. For more information about exporting questionnaire responses, see Export questionnaire responses to a spreadsheet.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Additional assessment actions

The TPR manager may need to reopen an assessment because there's new information available that impacts the engagement or some other change has occurred. For more information, see Why you conduct due diligence.

If the TPR manager must gather more information from an engagement, they can send out an additional questionnaire or document request by reopening an assessment and doing the following actions:

1. Navigate to the Due diligence request record page by selecting the relevant **DDR** number.
2. View the related third-party risk assessment by selecting the **VRA** number on the **Third-party risk assessment** tab.
3. Select **Re-open**.

The due diligence request state updates from Ready for TPRM approval to Due diligence. The TPR manager can request questionnaires and document requests as needed. For more information, see Reopen an assessment.

If the TPR manager doesn't require an assessment for an ongoing engagement or requires a quick close for onboarding or renewing an engagement, they can cancel an assessment by doing the following actions:

1. Navigate to the Due diligence request record page by selecting the relevant **DDR** number.
2. View the related third-party risk assessment by selecting the **VRA** number on the **Third-party risk assessment** tab.
3. Select **Cancel**.

Even if one or all assessments are canceled, the due diligence request proceeds to the Approval process.

## Issues and tasks

The role of TPR manager [sn_vdr_risk_asmt.vendor_risk_manager] or TPR assessor [sn_vdr_risk_asmt.vendor_assessor] is required to create and manage both tasks and issues.

The TPR managers or assessors can create tasks to help ensure that a team member or the third-party contact responds to concerns about the questionnaire responses or requested documents. They can manage existing tasks to verify that the assigned team member or third-party contact responds to a task and updates it as needed. For more information about creating and managing issues, see Create a task for a third party or engagement and Manage a task for a third party or engagement.

The TPR managers or assessors can create an issue to help ensure the teams concerns about a third party or engagement are remediated. They can also manage the existing issues to verify that they're understood, shared with the correct persons, and are acted on as needed. For more information about creating and managing tasks, see Create an issue for a third party or engagement and Manage issues.

## Respond to an Inherent Risk Questionnaire (IRQ)

Respond to an IRQ that has been assigned to your queue. Your responses to the questionnaire help determine if the process moves forward and can affect which questionnaires are sent to the third party or engagement.

### Before you begin

Role required: snc_internal

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

When someone in your organization creates a due diligence request, the owner of the overall due diligence process specifies who should respond to that initial IRQ. As an IRQ assessor, you receive an email that contains the links to the assigned questionnaires, the name of the related assessment, and the deadline. This information is also provided as part of the questionnaire in Employee Center. For more information, see Requesting third-party risk due diligence and Due diligence workflow.

**Note:** When a request is created, the system alerts the initial due diligence requester and all users in the Due diligence request assignment group. A member of the group can assign a Third-party risk (TPR) manager or TPR assessor to act as the owner of the request.

### Procedure

1. Navigate to **All** > **Self-Service** > **Employee Center** to open your Employee Center.
2. In the My active items pane, select **Surveys**.
3. Answer all relevant questions in the questionnaire and then select **Submit**.

Related topics

Why you conduct due diligence

## Review responses to external questionnaires

Third-party contacts use the Third-party portal to complete assessments and collaborate with the TPR manager in the comments section for each question. When assessments reveal gaps, the TPR manager or the TPR assessor can generate an issue or task. In addition, the Vendor Management Workspace application can auto-generate issues.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_assessor

### About this task

If the TPR manager or TPR assessor decides that an assessment response is unsatisfactory, they can return some of the questions or document requests in the assessment. Incorrect answers to questions can automatically generate issues, or issues can be generated manually from the question. The comments identify the issues to the third-party contact.

To enable TPR assessors to modify responses, configure the **Allow TPR assessors to modify responses in third-party questionnaires** [`sn_svdp.allow_assessor_edit`] system property. You can set the following options:

- Enable TPR assessors to answer questions or modify responses (default)
- Enable TPR assessors to modify responses
- Do not enable TPR assessors to answer questions or modify responses

See Configure TPRM properties.

### Procedure

1. In the Vendor Management Workspace, click the list icon (  ) and then navigate to **Vendor risk assessments** > **Open assigned to me**.
2. Open an assessment that is in the **Responses Received** state.
3. On the **Questionnaires** or **Document Requests** tab, click **View Responses** and then fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Vendor's Response form

| Field | Description |
|---|---|
| Reviewer comment | Text that provides internal information about the state of responses. |
| Show Follow-ups | Select the check box to display only questions that were flagged as needing a follow up (the **Follow up** check box was selected when the assessment was returned to the third-party for updates). |
| Show incorrect and un-scored responses | Select the check box to display only questions with an incorrect answer or for which no response was given. |
| Hide comments | Select the check box to hide all **Comment** text boxes. |
| Include this question when creating an issue | Select the check box to indicate that you want to create an issue dealing with this question. You can add an **Internal comment**.<br>**Note:** If you have already created an issue for a question, the field is disabled to prevent you from creating an additional issue for the question. |
| Follow up | Select the check box to make the external comment visible to the third party. |
| Comment for vendor | Select the check box to add an **External comment** for the third party. |

4. After you review the assessment and add comments, perform one of the following steps.

| Choice | Description |
|---|---|
| To generate issues associated with each question | Click **Create Issue**. A message with the issue number appears, and each question with an issue shows an icon to indicate that you cannot create a new issue for the question. The indicator is removed when the issue is closed or cancelled. |
| To resubmit the assessment to the vendor | Click **Return to Vendor**.<br>If the assessment schedule might be affected, you can extend the term by adjusting the number of days in the **Return questionnaire** window. |
| To add or review in the questionnaire | Click the **Notes and Comments** tab. |

## Reopen an assessment

Reopen an assessment to send out more questionnaires and document requests to collect required additional information from the third party or engagement.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_vdr_risk_asmt.vendor_assessor or sn_vdr_risk_asmt.vendor_risk_manager

### About this task
As the TPR manager, TPR assessor, or owner of the due diligence request, you may reopen an assessment due to an internal stakeholder request or if new information impacts the engagement. You can reopen an assessment after the due diligence request has gone through any of the following processes: due diligence, approval, or contract. The due diligence request must be in the Closed state before you can reopen an assessment. After reopening the assessment, you can select additional questionnaires and document requests to send from the Questionnaires and Document requests tabs.

### Procedure

1. In the Vendor Management Workspace, select the list icon (  ) and then navigate to **Due diligence requests** > **All requests**.
2. Select the relevant **DDR** number.
3. View the related Third-party risk assessments by selecting the **VRA** number on the **Third-party risk assessment** tab.
4. Select **Re-open**.

## Create an issue for a third party or engagement

Create an issue to help ensure that your concerns about a third party or engagement are remediated.

### Before you begin
Role required: sn_vdr_risk_asmt.vendor_risk_manager or sn_vdr_risk_asmt.vendor_risk_admin

### About this task
In an iterative process, before the TPR manager closes an assessment, the TPR manager can generate non-compliance issues and tasks. The TPR manager communicates with the TP contacts by using comments to close the issues and tasks. The TPR manager can also assign different TP contacts as needed.

### Procedure

1. In the **Quick actions** box on the TPRM home page (  ), select **Create issue**.
2. Optional: Select a template to fill in several fields on the form.
   You can filter the template list and add templates to your custom **My templates** list.
3. Fill in the form and then select **Save**.

#### Third-party risk issue form

| Field | Description |
|---|---|
| Name | Helpful tag for the template. The field might be filled in by a template. |
| Description | Text that helps others to understand the issue. |
| Number | For each issue, the system auto-assigns a unique ID number that starts with the text **VRI**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Applies to | ◦ **Third party**: The issue applies to the parent third-party organization.<br>◦ **Engagement**: The issue applies to the engagement. |
| Third party | Third party with which the issue is associated. |
| Assessment | Assessment with which the issue is associated. |
| State | The state of an issue is updated as you perform actions that are associated with the issue. The workflow chain along the top of the **Risk overview** tab identifies the current state of the issue. See Manage issues. |
| Priority | Specify the priority. The value appears in all reports that include the issue. |
| Assignment group | |
| Assigned to | User that is responsible for managing and closing the issue. |
| Third-party contact | Contact at the third party with which the issue is associated. |
| Watch list | Add other users to help ensure that they see updates in the issue state and other values. |
| Visible in vendor portal | Option to display the issue to the vendor contacts in the Third-party portal. |
| **Recommendations section** | |
| Recommendation | ◦ Third party to remediate: You expect that the TP contact will remediate the issue so you can close it.<br>◦ Accept issue: You determine that the risk associated with issue is acceptable and requires no further action.<br>◦ Request additional information: You will request additional information from the TP contact.<br>The field might be filled in by a template. |
| Explanation | The field might be filled in by a template. |

If **Visible in vendor portal** is selected, then the third-party contact is alerted to the issue.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Result**
The highest priority issues are listed in the Issues by priority section of the Home page. The **Assigned to** user can manage the issue on the tabs of the Issue management page. See Manage issues.

Related topics

TPRM Home page

## Manage issues

Verify that an issue that is associated with a risk assessment is understood, communicated to the appropriate persons, and is acted on as needed.

**Before you begin**
Role required: sn_vdr_risk_asmt.vendor_risk_manager or sn_vdr_risk_asmt.vendor_risk_admin

**Procedure**

1. Use either of the following methods to start the process:
   - On the TPRM **Home** page (  ), the highest priority issues are listed in the **Issues by priority** section. Select an issue name to view the **Risk overview** tab on the Issue page.
   - On the **List** page (  ), select the issue name from one of the lists in the **Issues**section to view the **Risk overview** tab on the Issue page.

   **Note:** For each issue, the system auto-assigns a unique ID number that starts with the text **VRI**. The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on.

2. Optional: Select an action.
   - Select **Discuss** to send a message to other users. The message is recorded in the **Activity** section of the **Details** tab.
   - select **Create task** to create a task. See Create a task for a third party or engagement.
   - Select **Save** to save any change you made to a value on any tab.
   - select **Delete** to delete the issue record.
3. Open the appropriate tab.

   On each tab, the Third-party overview section displays general details for the third party.

   Risk overview tab for an issue
   - The workflow chain along the top identifies the current state of the issue. The state is updated as you perform actions that are associated with the issue.
   - Tasks section: Lists associated tasks and displays the count and status of tasks. For each issue, the system auto-assigns a unique ID number that starts with the text **VRI**. The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on.
   - Tasks by planned end date section: Helps you to identify tasks that need urgent attention.
   - Third-party overview section: General details for the third party.

   Details tab for an issue

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Third-party risk issue section: General information on the third party and recommended actions for the issue.

- The **Compose section** on the **Details** tab enables you to permanently add text to the record. The Activity section is updated with any actions on issues and tasks, submissions to TP contacts, and also with work notes and comments that users add to the record. Add text in the following fields as needed:
  - **Work notes (Private)**: Information about the third-party risk assessment. Work notes are visible only to internal users who are assigned to the process.
  - **Comments**: Comments about the third-party risk assessment are visible both to internal users and to third-party contacts.

Tasks tab for an issue

The tab displays information for tabs that are associated with the issue. Select a task number to open the task in the task management page. Select **New** to create a task. See Create a task for a third party or engagement.

Questions tab for an issue

The tab displays a list of the questions that are associated with the issue. Select a question to view the question definition and current response.

## Create a task for a third party or engagement

Create a task to help ensure that a user at your organization or the third-party contact responds to your concerns about questionnaire responses or requested documents during the due diligence process.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager or sn_vdr_risk_asmt.vendor_risk_admin

### About this task

In an iterative process, before the TPR manager closes an assessment, the TPR manager can generate non-compliance issues and tasks. The TPR manager communicates with the TP contacts by using comments to close the issues and tasks. The TPR manager can also assign different TP contacts as needed.

### Procedure

In the **Quick actions** box on the TPRM home page (  ), click **Create task**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Create New Third-party risk task

Details

## Third-party risk task

Short description *

Description

Number: VRT0003002

State: Open

Applies to: Third-party

Priority: 4 - Low

Third-party

Assigned to: (Empty)

Assessment

Third-party contact

Issue

Watch list

Visible in vendor portal

## Task schedule

Planned duration

| Days | Hours | Minutes | Seconds |
|---|---|---|---|
| 1 | 0 | 0 | 0 |

Actual duration

| Days | Hours | Minutes | Seconds |
|---|---|---|---|
| 0 | 0 | 0 | 0 |

Planned start date: 2023-07-19 20:06:55

Actual start date: YYYY-MM-DD HH:mm:ss

Planned end date: 2023-07-19 20:06:55

Actual end date: YYYY-MM-DD HH:mm:ss

Closed by

Created: —

Updated: —

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Third-party risk task form

| Field | Description |
|---|---|
| Short description / Description | High-level and detailed information about the issue that needs to be resolved and the method for resolving it. |
| Number | For each task, the system auto-assigns a unique ID number that starts with the text **VRT**.<br><br>The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Applies to | • **Third party**: The task applies to the parent third-party organization.<br>• **Engagement**: The task applies to the engagement. |
| Third party | Third party with which the task is associated. |
| Assessment | Assessment with which the task is associated. |
| Issue | Issue with which the task is associated. |
| State | |
| Priority | Specify the priority. The value appears in all reports that include the task. |
| Assigned to | User that is responsible for managing and closing the task. |
| Third-party contact | Contact at the third party with which the task is associated. |
| Watch list | Add other users to help ensure that they see updates in the task state and other values. |
| Visible in vendor portal | Option to display the task to the vendor contacts in the Third-party portal. |
| **Task schedule section** | |
| Planned duration / Actual duration | The time period that you expect the task to require and the actual duration that is calculated from the actual start and actual end dates. |
| Planned start date / Planned end date | Expected start and end dates for the task. |
| Actual start date / Actual end date | Actual start and end dates for the task based on the first action and the date the task was closed. |
| Closed by | User who closed the task (typically the owner — the **Assigned to** user). |
| Created / Updated | Dates that the task was saved and date of the latest change. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Manage a task for a third party or engagement

Verify that the **Assigned to** user at your organization or the third-party contact responds to a task and update the state of the task as needed.

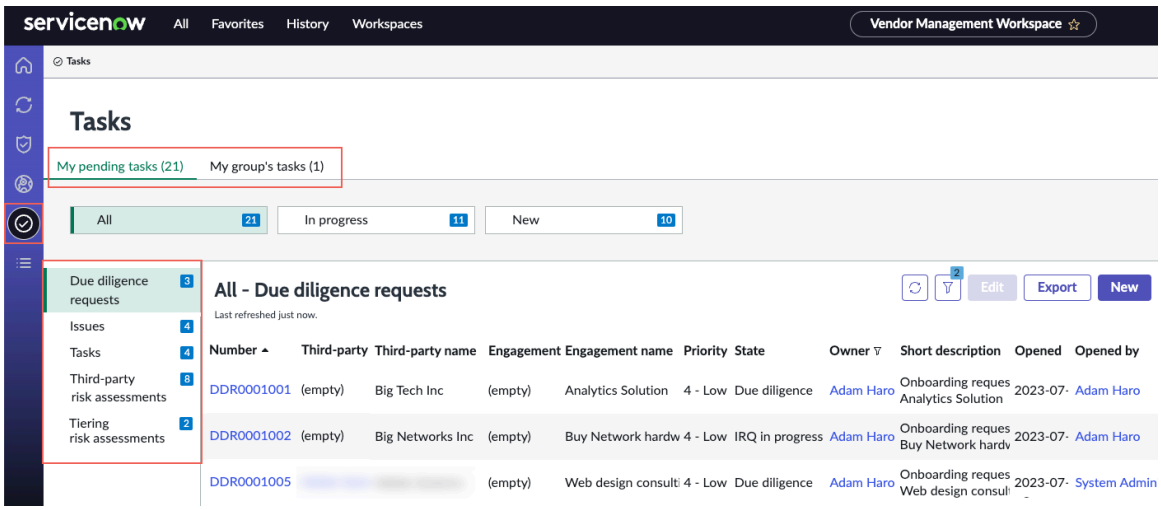
### Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager or sn_vdr_risk_asmt.vendor_risk_admin

### Procedure

1. Select **Workspaces** > **Vendor Management Workspace** and then select the **Risk** tab to open the workspace to the home page and then select the Task icon ( ).
2. On either the **My pending tasks** or **My group's tasks** tab, select **Tasks**, and then select the task number.

**Note:** The other options in the list (**Due diligence requests**, **Issues**, and so on) also enable you to select a task to work on.




### Third-party risk task form

| Field | Description |
|---|---|
| Short description / Description | Text that explains and clarifies the intent of the task for users. |
| Number | For each task, the system auto-assigns a unique ID number that starts with the text **VRT**.<br><br>The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Applies to | ◦ **Third party**: The task applies to the parent third-party organization.<br>◦ **Engagement**: The task applies to the engagement. |
| Third party | Third party with which the task is associated. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Assessment | Assessment with which the task is associated. |
| Issue | Issue with which the task is associated. |
| State | |
| Priority | Specify the priority. The value appears in all reports that include the task. |
| Assigned to | User that is responsible for managing and closing the task. |
| Third-party contact | Contact at the third party with which the task is associated. |
| Watch list | Add other users to help ensure that they see updates in the task state and other values. |
| Visible in vendor portal | Option to display the task to the vendor contacts in the Third-party portal. |
| **Task schedule section** | |
| Planned duration / Actual duration | The time period that you expect the task to require and the actual duration that is calculated from the actual start and end dates. |
| Planned start date / Planned end date | Expected start and end dates for the task. |
| Actual start date / Actual end date | Expected start and end dates for the task based on the first action and the date the task was closed. |
| Closed by | User who closed the task (typically the **Assigned to** user). |
| Created / Updated | Dates that the task was saved and date of the latest change. |

## Export questionnaire responses to a spreadsheet

Export received or returned questionnaires to Microsoft Excel spreadsheets. This option enables you to use the spreadsheet environment to review questions and answers.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_assessor

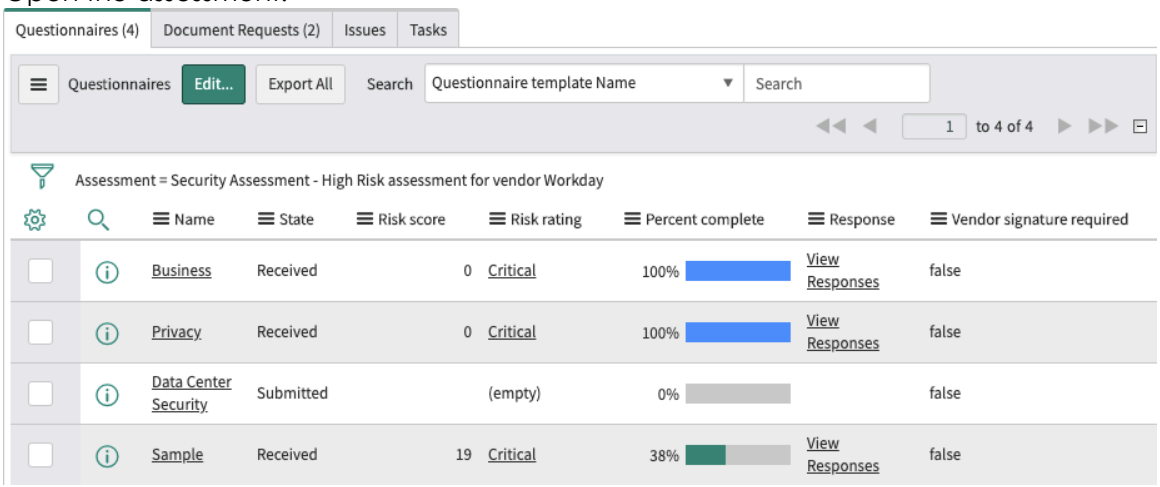
### About this task

You can export only questionnaires in the received or returned state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Open the assessment.



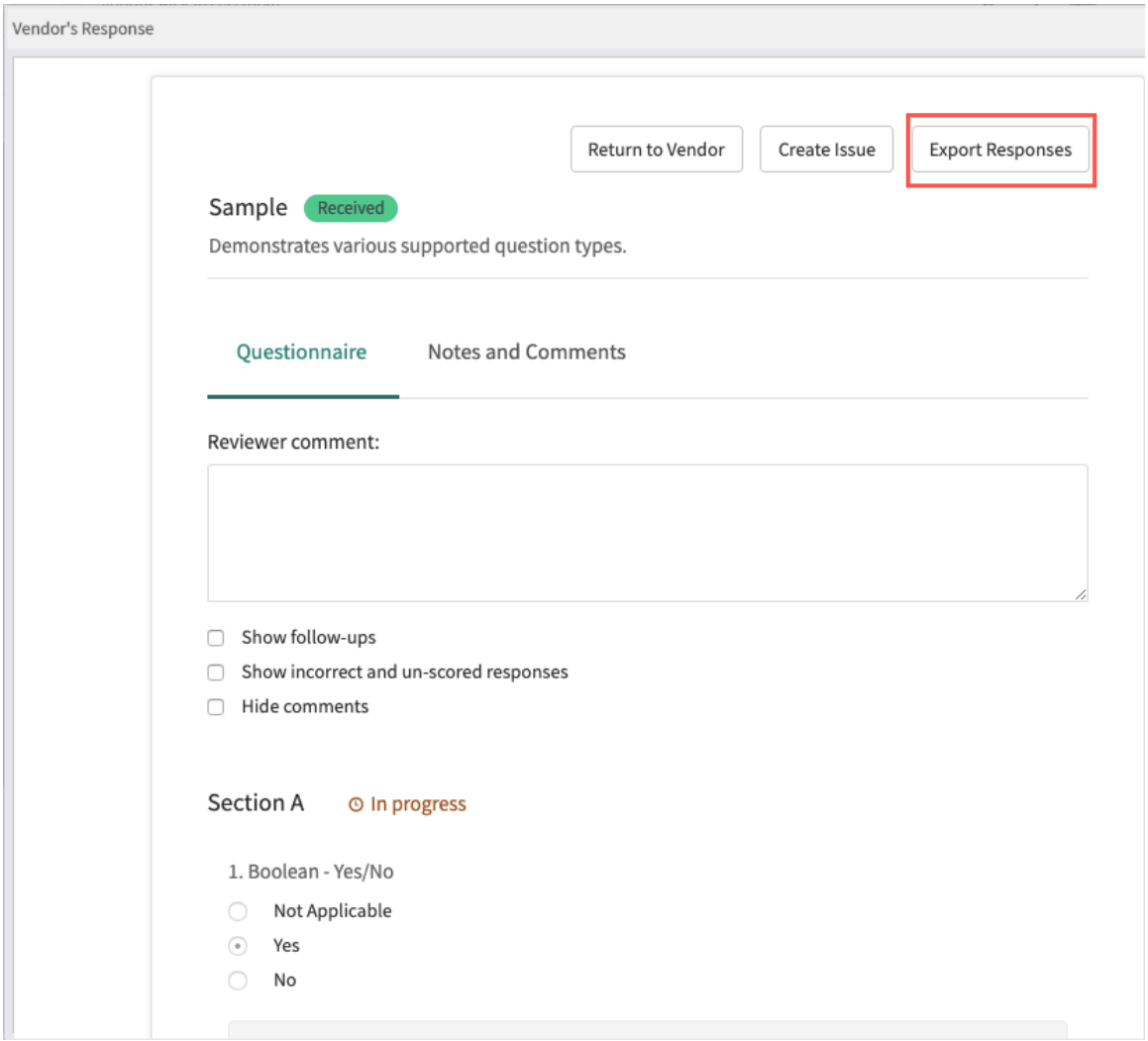

2. Scroll to the **Questionnaires** related list and then use one of the following methods to export the questionnaire.

   - To export a single questionnaire:

     a. Click **View Responses** and then click **Export Responses**.

     b. Click **Export**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




◦ To export more than one questionnaire:

**a.** Select the check boxes for the questionnaires, then select **Export Questionnaire** from the **Actions on selected rows** list.

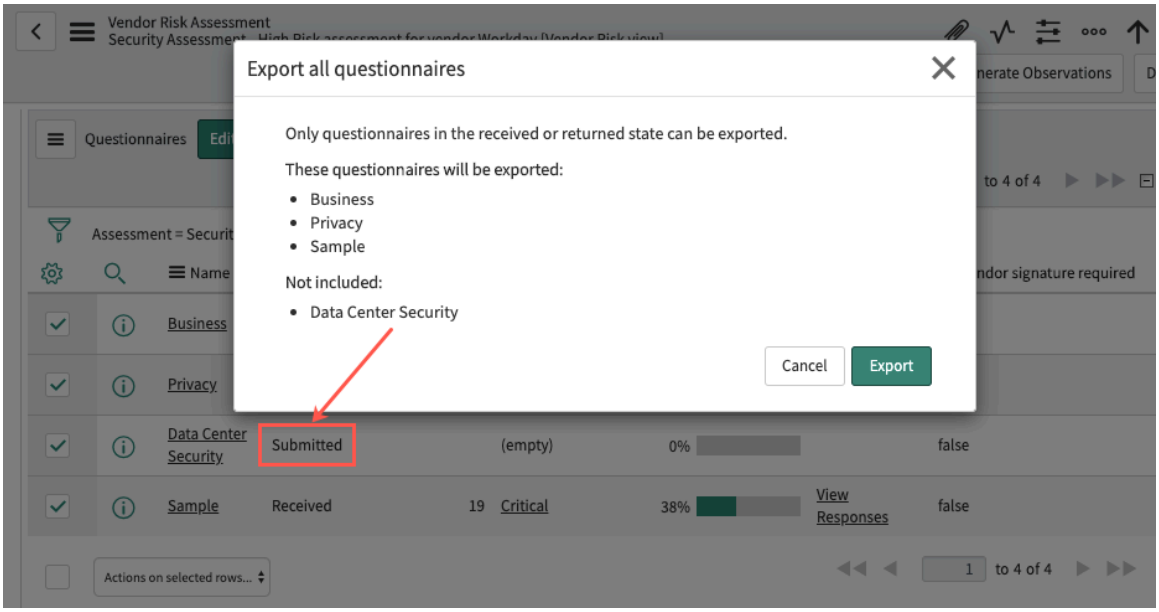
**b.** Click **Export**.

◦ To export all listed questionnaires:

**a.** Click **Export All**.

**b.** A pop-up lists the questionnaires to be exported. In the example, the **Data Center Security** questionnaire is not exported because it is not in the received or returned state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**c.** Click **Export**.

The system generates a compressed file that contains a separate Excel file for each questionnaire. Exported files use the following file naming convention: `<assessmentName> - <questionnaireName>.xlsx`.

The **Assessment details** tab in a spreadsheet shows the name and state of the assessment, the planned and completion dates, an signatory details. Each **Section** tab displays the question data for the assessment categories.

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | Serial number | Question | Data type | Answer choices | Correct answers | Actual answers |
| 2 | 1 | 1. Boolean - Yes/No | Yes/No | Yes No | Yes | Yes |
| 3 | 2 | 1.1. Dependent Question | Yes/No | Yes No | Yes | No |
| 4 | 3 | 1.2. Dependent Question | Yes/No | Yes No | Yes | Yes |
| 5 | 4 | 1.3 Dependent Question - Mandatory | Yes/No | Yes No | Yes | Yes |
| 6 | 5 | 2. Boolean | Checkbox | Checked Unchecked | Checked | Unchecked |
| 7 | 6 | 3. Attachment | Attachment | | | |
| 8 | 7 | 4. Choice | Choice | Choice 1 Choice 2 Choice | Choice 4 | Choice 1 |
| 9 | 8 | 5. Date | Date | | | |
| 10 | 9 | 6. Date and Time | Date/Time | | | |

Assessment details | Section A | Section B | Section C | Section D

# Monitoring your third-party risk

Use the Third-party Risk Management application to monitor potential risks associated with your third-party relationships. An ongoing monitoring process can help with regularly assessing the third party's performance and adherence to agreed-upon terms.

## Ongoing monitoring and review

Using the Vendor Management Workspace, Third-party risk (TPR) managers [sn_vdr_risk_asmt.vendor_risk_manager] can regularly assess the third party's performance and adherence to agreed-upon terms.

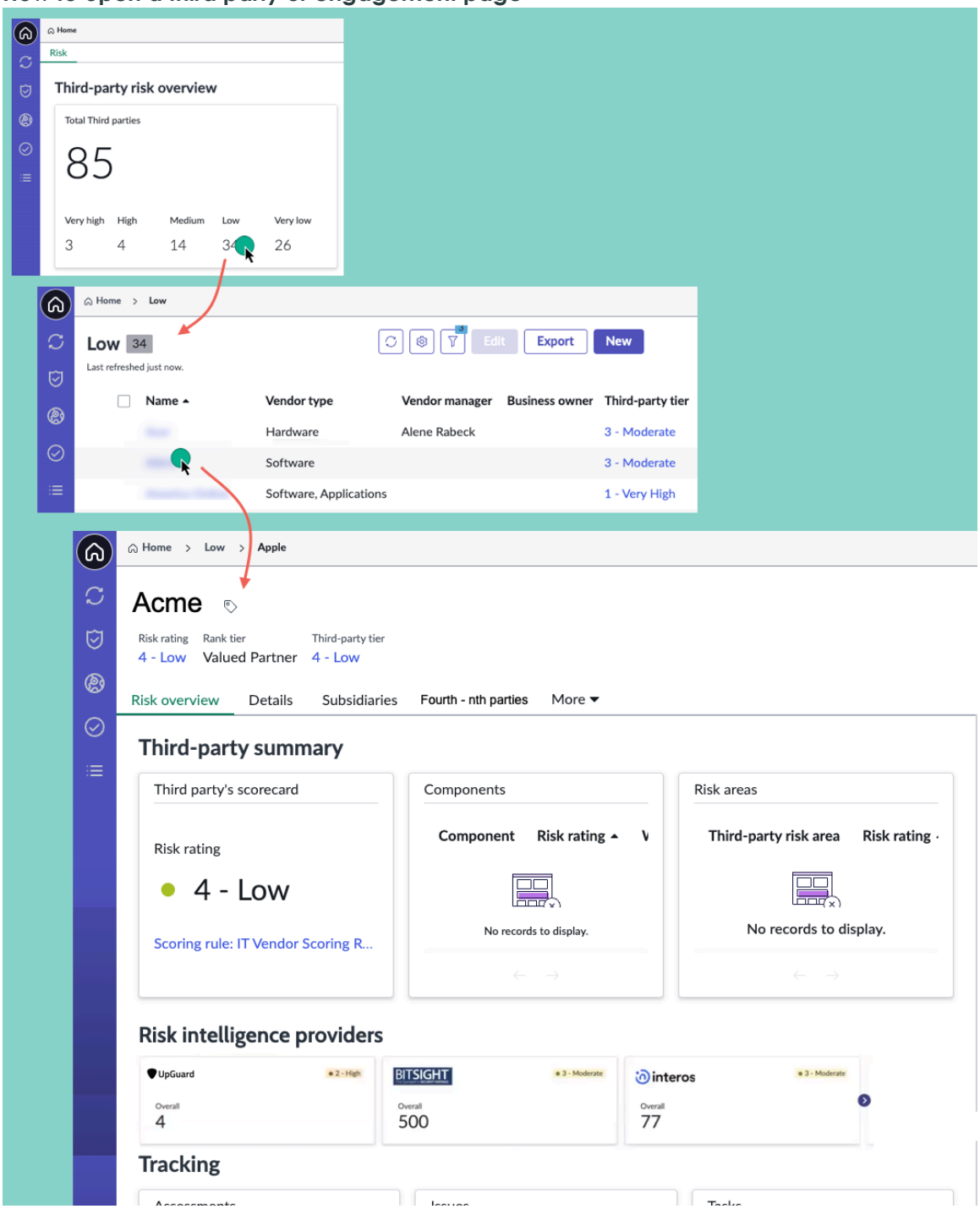
You can view the risk reports for all third parties and engagements by navigating to the workspace home page. Navigate to **Workspaces** > **Vendor Management Workspace** and

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

then select the **Risk** tab to open the workspace to the home page. For more information, see Viewing third-party risk reports.

You can view the status and all current information for a third party or engagement by navigating to the third party or engagement's page. Navigate to **Workspaces** > **Vendor Management Workspace**. On the **Risk** tab, select . As shown in the following example, you can select any number in the Third-party risk overview section to open a list of third parties or engagements with that value and select a third party or engagement.

### How to open a third party or engagement page




For more information, see Get an overview of a third party or engagement.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can view the status of the following due diligence processes from the Due diligence request record page:

- Request process
- Inherent Risk Questionnaire (IRQ) process
- Third-party risk assessment process
- Approval process
- Contract risk process

You can access the Due diligence request record page by selecting the **DDR** number for any due diligence request. The page opens to the **Details** tab. Typically, you start from the TPRM Home page. For more information, see Monitoring the due diligence request process.

The Vendor Management Workspace is designed for users with the TPR manager (Third-party risk manager) [sn_vdr_risk_asmt.vendor_risk_manager], TPR assessor (Third-party risk assessor) [sn_vdr_risk_asmt.vendor_assessor], and Third-party assessment reviewer [sn_vdr_risk_asmt.vendor_assessment_reviewer] roles.

## Managed Activity

You can view your managed activities for verification purposes with the Usage analytics activities [sn_vdr_risk_asmt_ua_activity] table. This read-only table stores a record whenever a managed activity occurs. You must have the Third-party assessment reviewer [sn_vdr_risk_asmt.vendor_assessment_reviewer] role to view this table. You can access the Usage analytics activities table by navigating to **All** > **Third Party Risk Management** > **Administration** > **Managed Activity Analytics**. For more information, see Tracking a managed activity.

**Note:** The Usage analytics activities [sn_vdr_risk_asmt_ua_activity] table is only available to those users that have purchased the Third-party Risk Management application and have access to the Due diligence management application. To see the instructions for downloading a GRC application from the ServiceNow® Store, see Download a GRC application from the ServiceNow Store for the first time.

## Get an overview of a third party or engagement

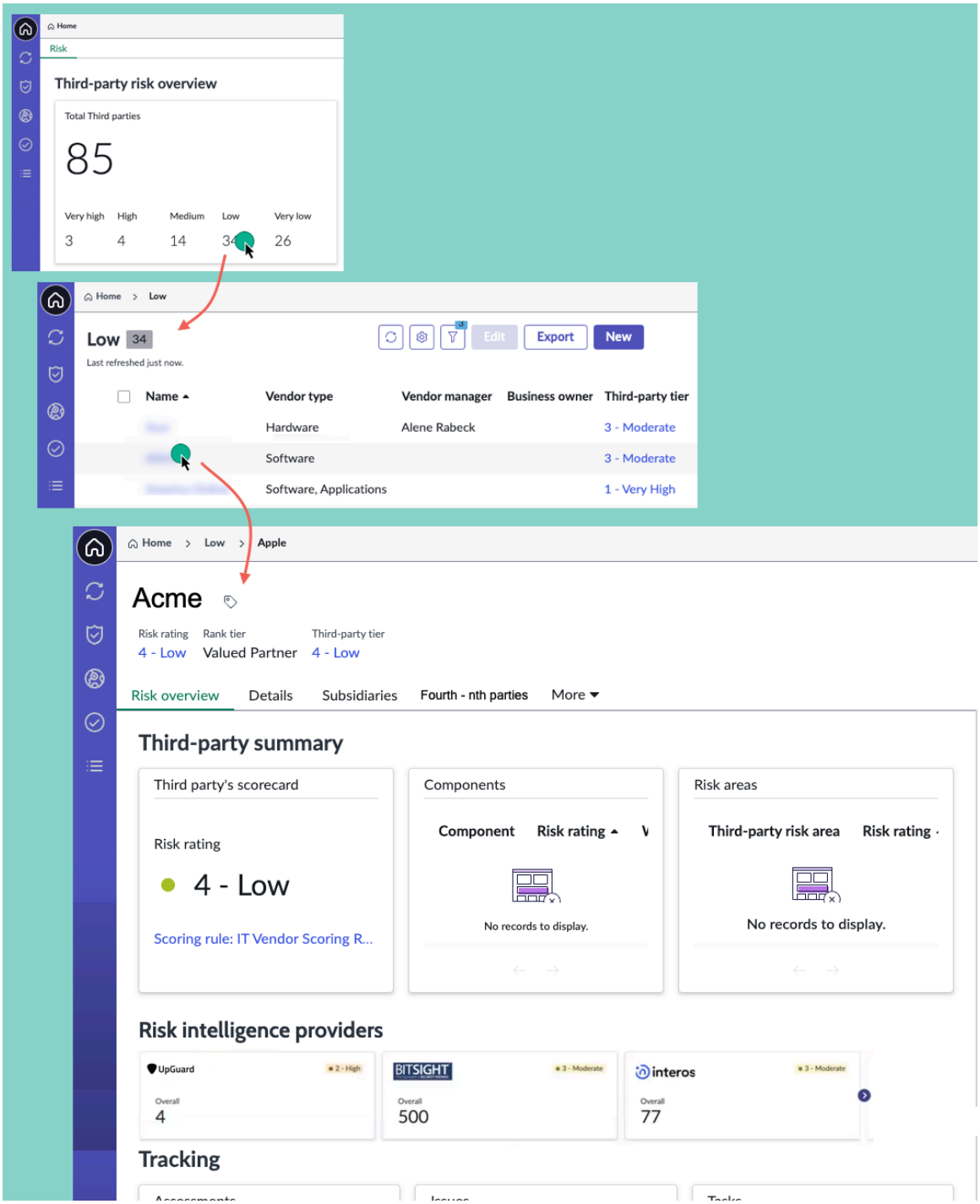
Use the engagement page to access all current information and status for a third party or engagement.

### Accessing third-party or engagement information

1. Select **Workspaces** > **Vendor Management Workspace**.
2. On the **Risk** tab, select  .
3. In the Third-party risk overview section, select any number in a box to open the list of third parties or engagements with that value.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select a third party name or engagement name and then select the appropriate tab.




## Information on the tabs for a third party or engagement

On most reports, you can select an item to view the underlying data.

Risk overview tab for a third party or engagement

The Risk overview tab displays third-party name and process information, summary reports, risk intelligence scores, and tracking data for issues and tasks. See Viewing summarized risk information for a third party or engagement.

Details tab for a third party or engagement

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **Details** tab displays overview and process tracking information and offers actions for managing the third party or engagement. See Viewing general information on a third party or engagement

Subsidiaries tab for a third party or engagement

The Subsidiaries tab displays overview information on subsidiaries of the third party. See Viewing information about third-party subsidiaries

Downstream suppliers tab for a third party or engagement

The **Downstream suppliers** tab displays overview information on fourth parties that the third party engages with. See Viewing information on fourth parties.

Risk intelligence scores tab

For DD requests, risk intelligence scores appear in a list. For an individual third party, a card displays the most recent score or rating and a link for each risk intelligence report. See Viewing risk intelligence scores.

### Viewing summarized risk information for a third party or engagement

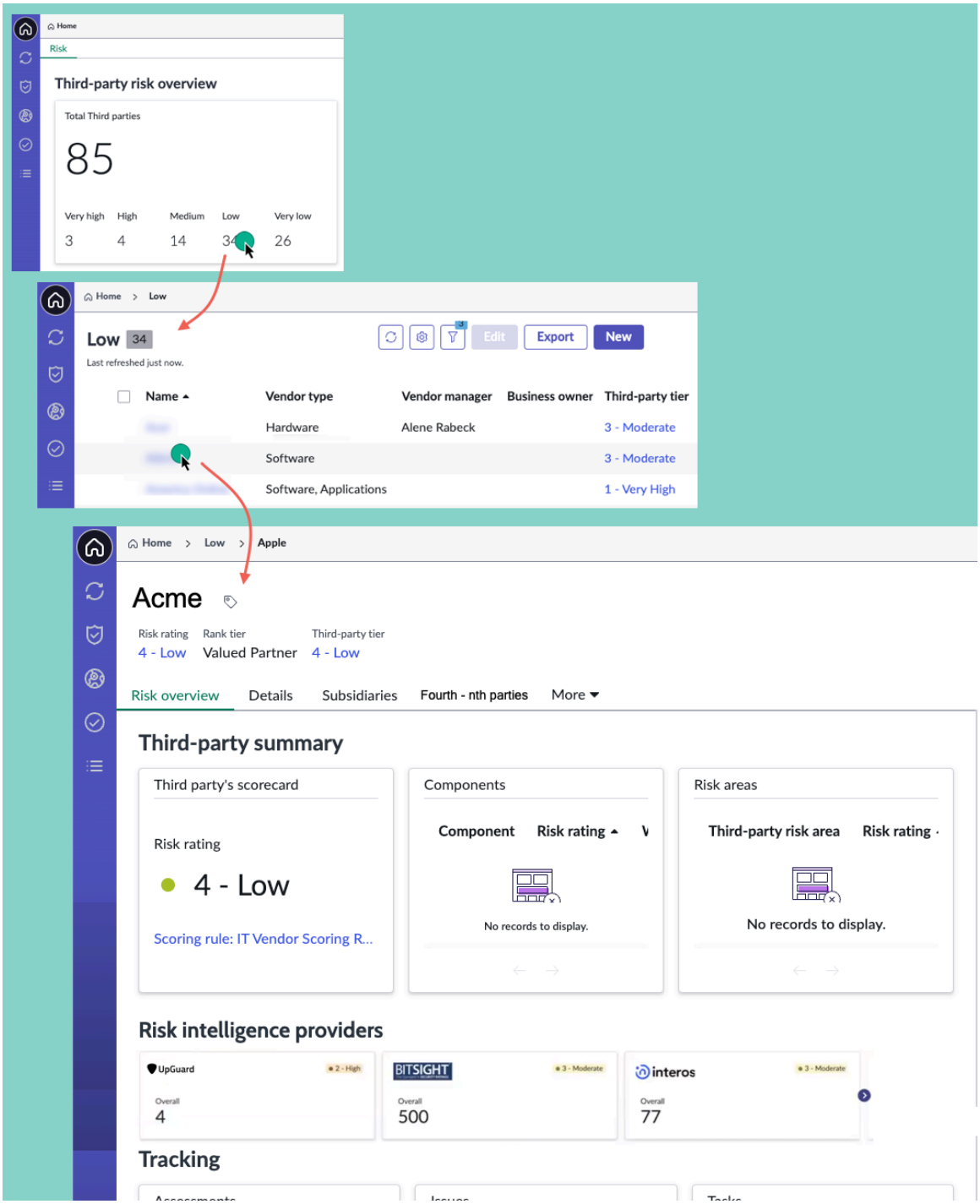
The Risk overview tab displays third-party name and process information, summary reports, risk intelligence scores, and tracking data for issues and tasks. On most reports, you can select an item to view the underlying data.

## Getting to the Risk overview tab

1. Select **Workspaces** > **Vendor Management Workspace**.
2. On the **Risk** tab, select  .
3. In the Third-party risk overview section, select any number in a box to open the list of third parties or engagements with that value.

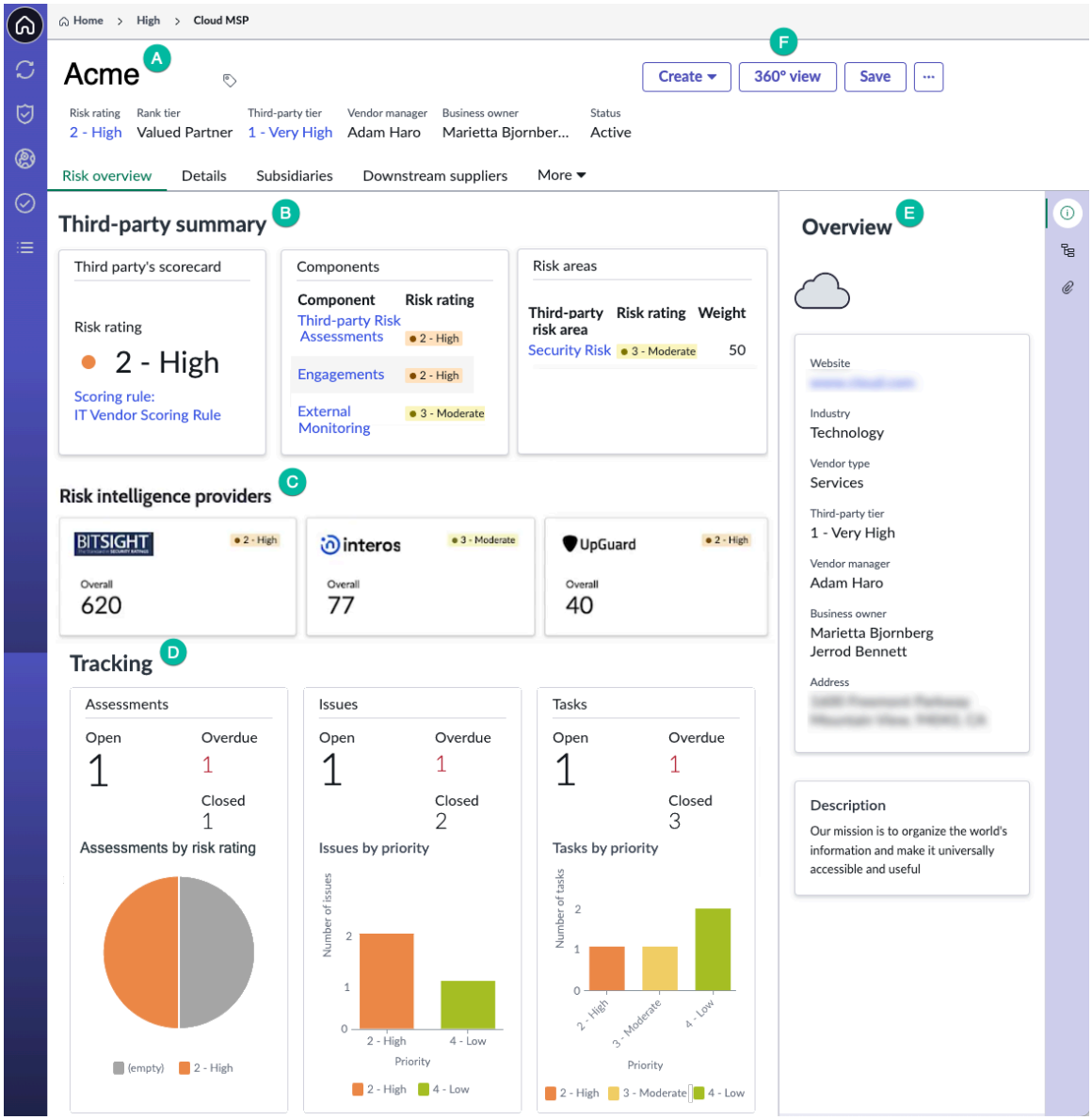
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**4.** Select a third party name or engagement name and then select the appropriate tab.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Information on the Risk overview tab




A: Name and process information

This section provides quick access to tier and contact information. Risk tiers are described in Third-party risk tiering assessments — Legacy process.

B: Third-party summary

Risk rating and scoring rules are described in Set up risk rating scales and scoring. Third-party risk components are external assessments, engagements, and subsidiaries. The component risk ratings are aggregated and are displayed as the **Risk rating** value on the **Third party's scorecard**.

C: Risk intelligence providers

Risk intelligence scores are described in Set up risk rating scales and scoring and Viewing risk intelligence scores.

D: Tracking

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Assessments: Counts of assessments in various process statuses. Select a number to view details.
- Issues: Issues are described in Create an issue for a third party or engagement and Manage issues.
- Tasks: Tasks are described in Create a task for a third party or engagementand Manage a task for a third party or engagement.

E: Overview

This section provides quick access to basic information about the third party.

F: Actions

- **Discuss**: Select **Discuss** to send a message to other users. The message is recorded in the **Activity** section of the **Details** tab.
- **Create**: Generate an issue or task. See Create an issue for a third party or engagement and Create a task for a third party or engagement.
- **360° view**: Visually explore the relationships between existing assessments, issues, tasks, product models, upstream, and downstream contacts that affect the selected third party. See 360° Relationship Visualization.
- **Save**: Save changes that you have made on the page.

### Viewing general information on a third party or engagement

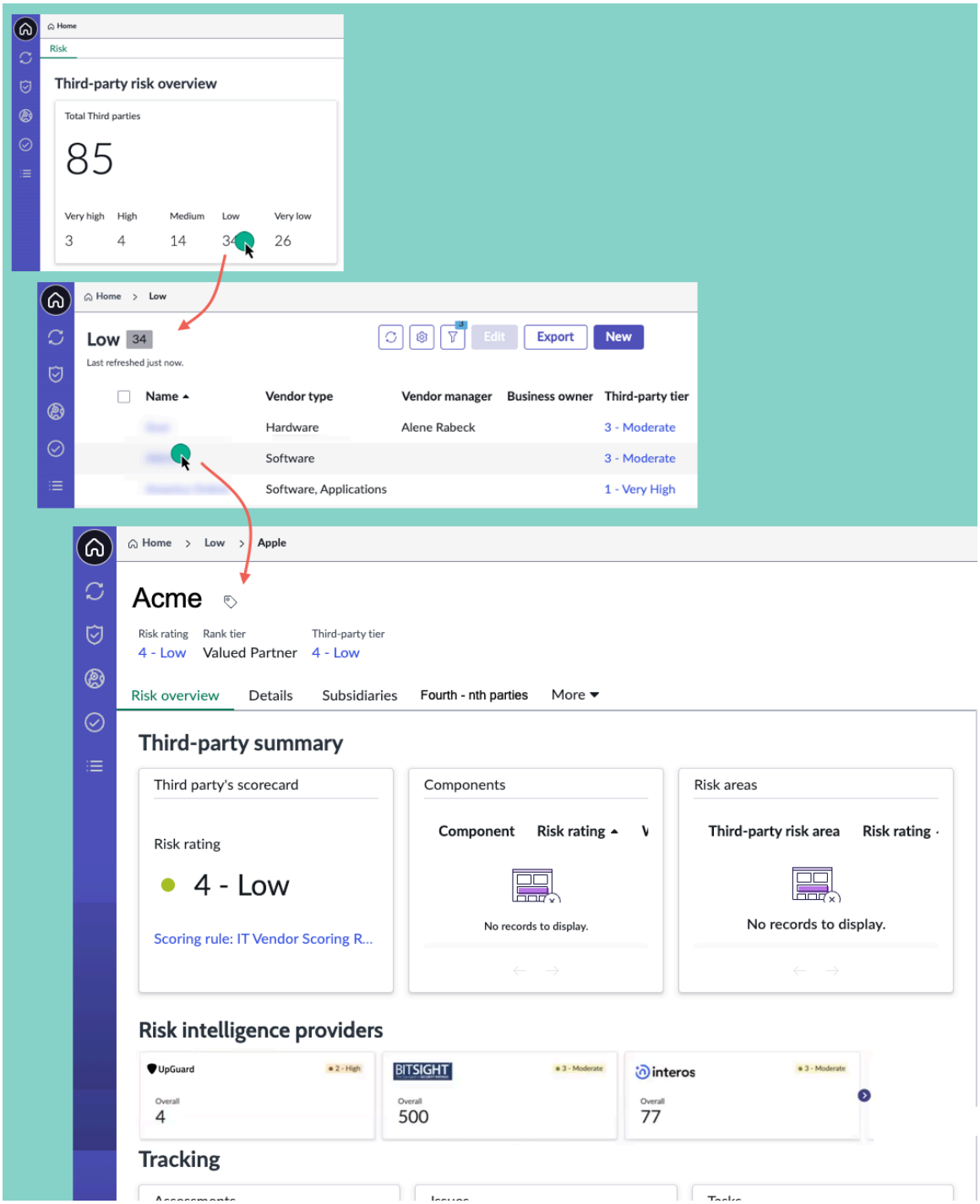
The **Details** tab displays overview and process tracking information and offers actions for managing the third party or engagement.  On most reports, you can select an item to view the underlying data.

## Getting to the Details tab

1. Select **Workspaces** > **Vendor Management Workspace**.
2. On the **Risk** tab, select  .
3. In the Third-party risk overview section, select any number in a box to open the list of third parties or engagements with that value.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select a third party name or engagement name and then select the appropriate tab.




For more information, see Due diligence request process management.

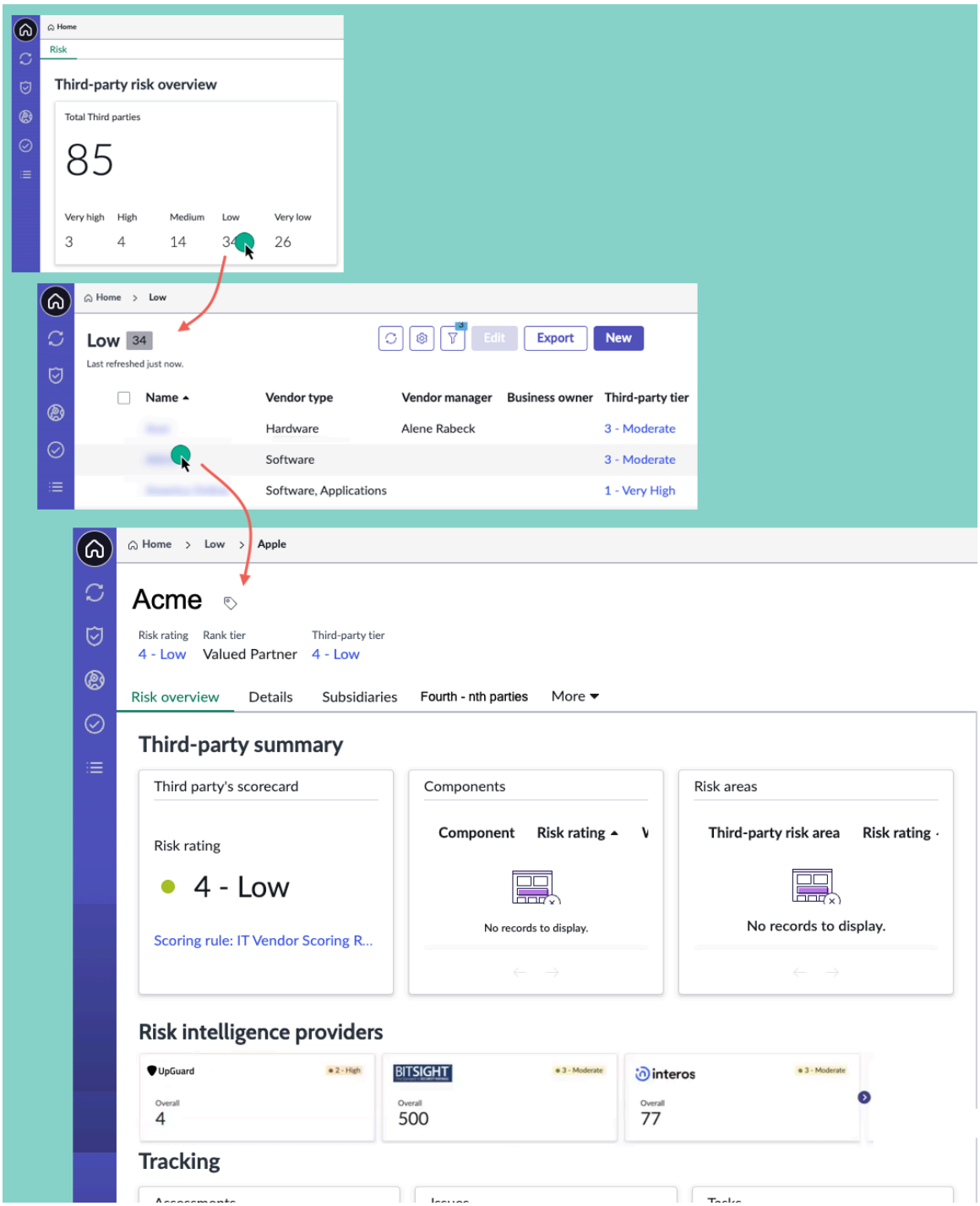
### Viewing information about third-party subsidiaries

The Subsidiaries tab displays overview information on subsidiaries of the third party. On most reports, you can select an item to view the underlying data.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Getting to the Subsidiaries tab

1. Select **Workspaces** > **Vendor Management Workspace**.
2. On the **Risk** tab, select  .
3. In the Third-party risk overview section, select any number in a box to open the list of third parties or engagements with that value.
4. Select a third party name or engagement name and then select the appropriate tab.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Viewing information on fourth parties

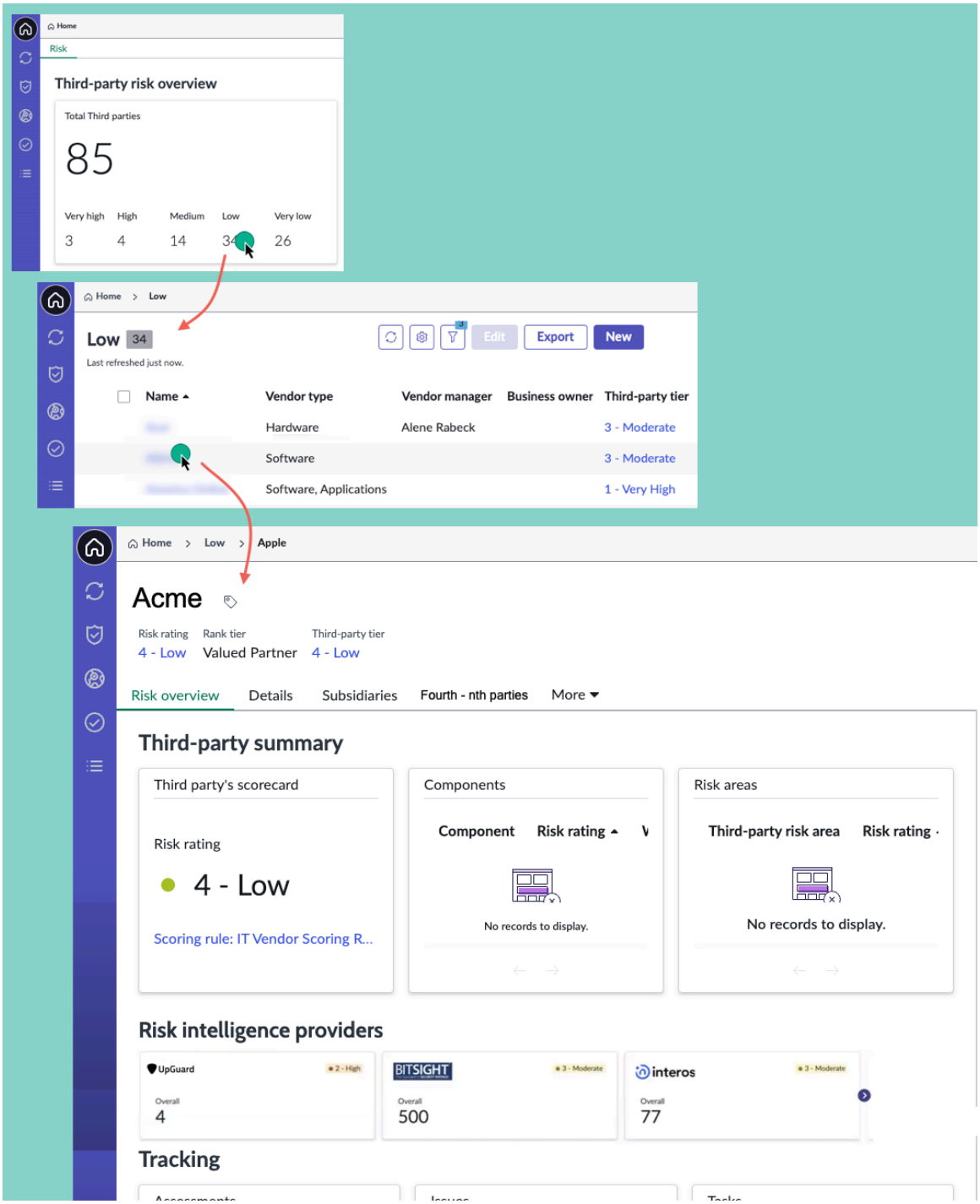
The **Downstream suppliers** tab displays overview information on fourth parties that the third party engages with.  On most reports, you can select an item to view the underlying data.

## Getting to the Downstream suppliers tab

1. Select **Workspaces** > **Vendor Management Workspace**.
2. On the **Risk** tab, select  .
3. In the Third-party risk overview section, select any number in a box to open the list of third parties or engagements with that value.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select a third party name or engagement name and then select the appropriate tab.




## Information on the Downstream suppliers tab

The name, website, and DUNS number for the fourth party are listed.

### Viewing risk intelligence scores

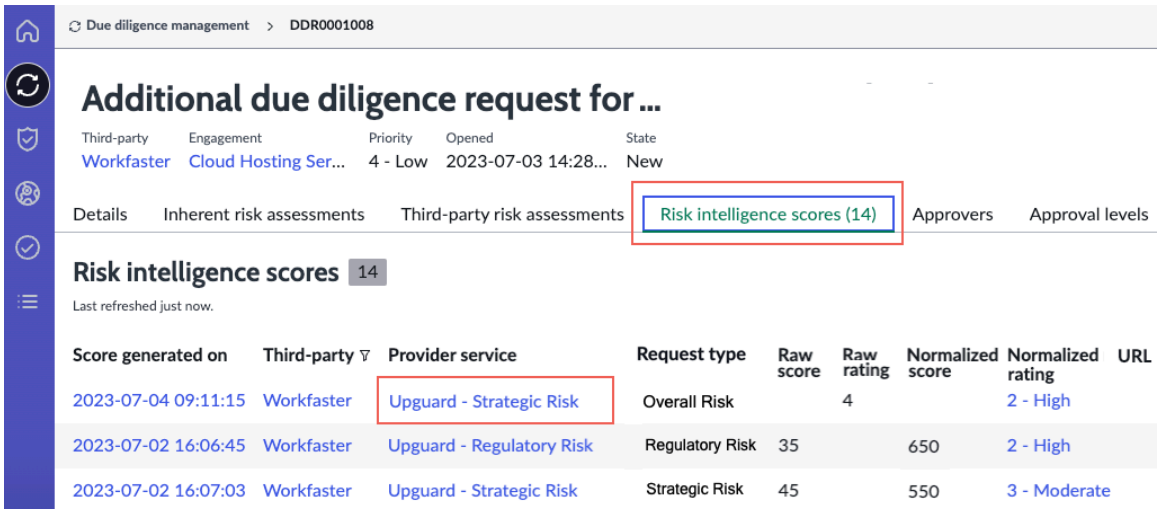
For DD requests, risk intelligence scores appear in a list. For an individual third party, a card displays the most recent score or rating and a link for each risk intelligence report.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Risk intelligence scores are described in Integrating scores from risk intelligence providers, Set up a risk intelligence provider service, and Add a risk intelligence score to risk data for a third party.

## Risk intelligence scores for DD requests

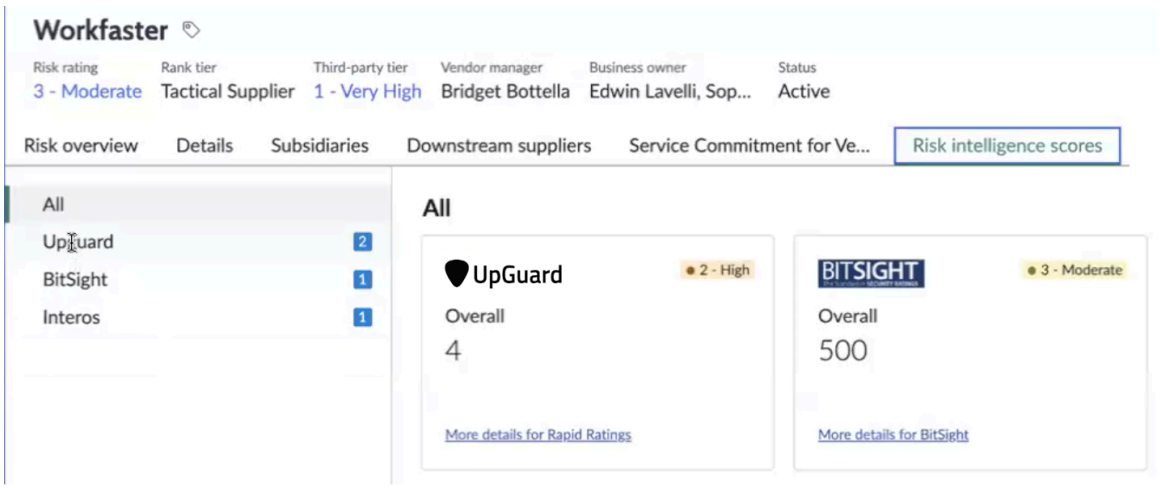
While viewing the data for a DD request, select the **Risk intelligence scores** tab to view the list of reports that risk intelligence providers have returned.




## Risk intelligence scores for a third party

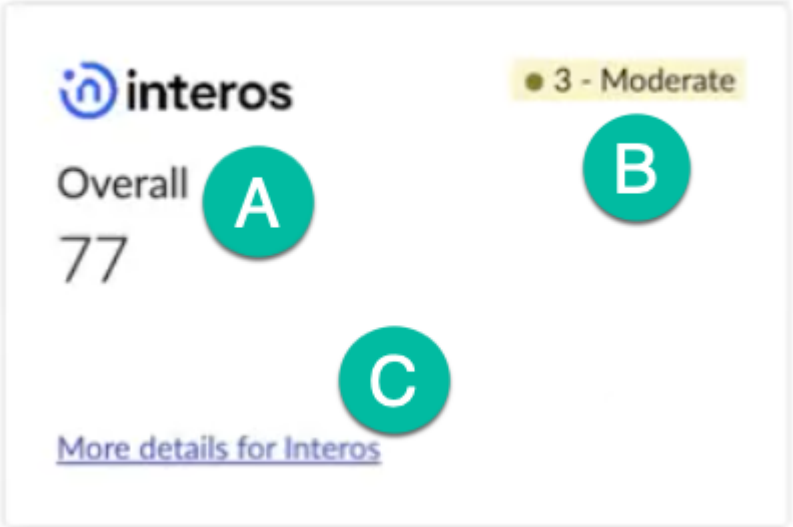
While viewing the data for a third party, select the **Risk intelligence scores** tab.

The list of risk intelligence providers that have returned data for the third party includes the count of scores that were associated with the third party. Click a number to view report details.




Each card displays the following information:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




- A. Overall value: The most recently added overall raw score or raw rating from the provider.
- B. Normalized risk rating. If you entered a numerical raw score or raw rating from the provider, then this is the computed normalized TPRM rating. You specified the mapping from the provider's values to the TPRM rating while configuring the provider service.
- C. Link to the report that the provider returned for your request for a risk intelligence score.

Related topics

Add a risk intelligence score to risk data for a third party

Set up a risk intelligence provider service

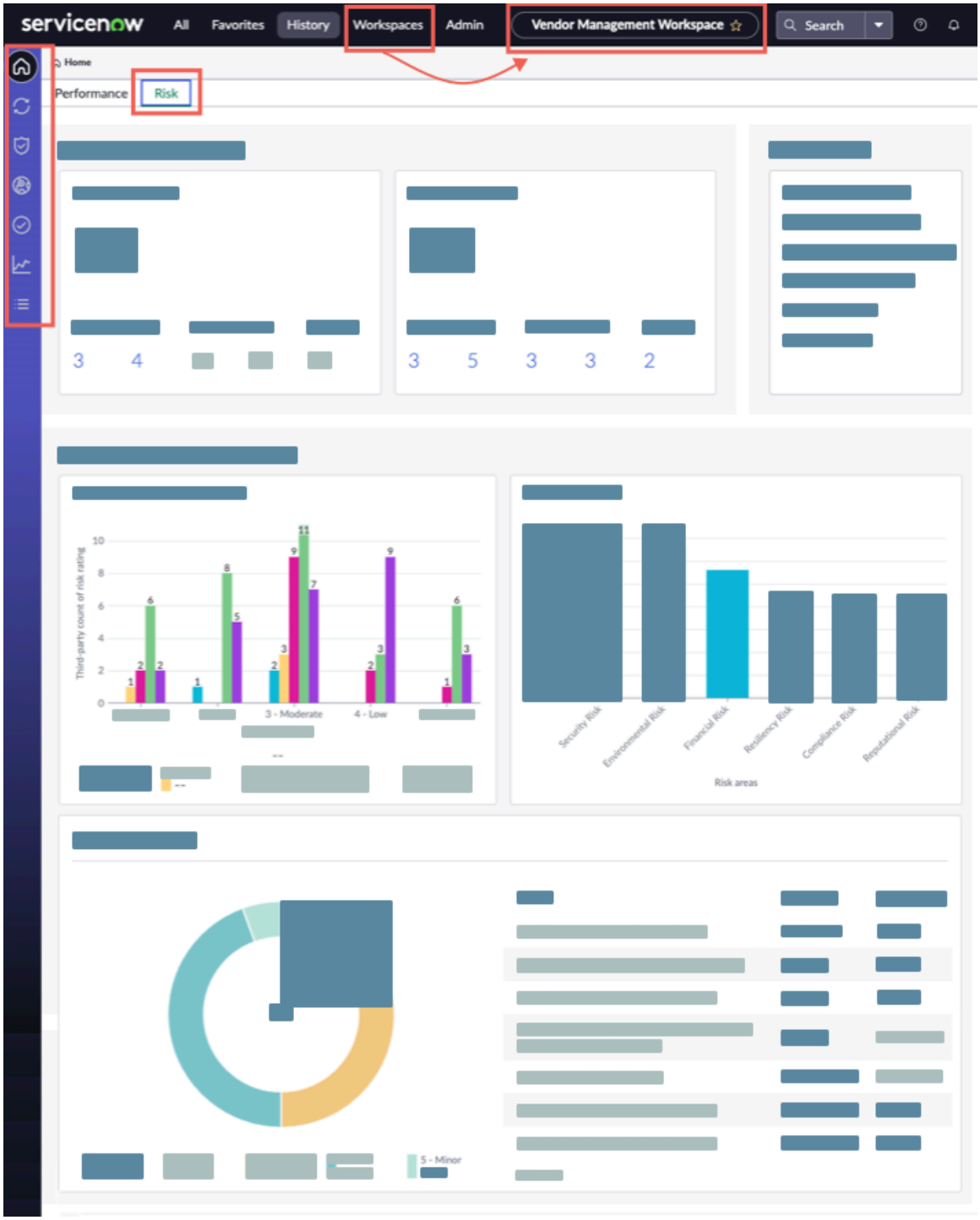
## Viewing third-party risk reports

Use the **Risk** tab on the Vendor Management Workspace to access and prioritize activities such as managing your portfolio of third parties, assessing third-party risk, and completing the remediation life cycle. The workspace enables automation that reduces the manual burden and costs of risk assessment.

## Navigating the Vendor Management Workspace

Select **Workspaces** > **Vendor Management Workspace** and then select the **Risk** tab to open the workspace to the home page. Each icon in the navigation panel opens a specialized page.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




Home page

The home page displays reports of important risk information and provides quick access to actions for TPR managers and TPR assessors. See TPRM Home page.

Due diligence management page

TPR managers and assessors use the due diligence management reports to track, prioritize, and manage their responsibilities. See TPRM Due diligence management reports.

Risk activity page

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The Risk activity page enables you to quickly identify assessments, issues, and tasks that need attention. See TPRM Risk activity page.

Risk concentration map page

The Risk concentration map page pinpoints the geographical locations of active third parties and engagements. You can configure filters to view particular risk ratings and engagement types. See TPRM Risk concentration map.

Task page

The task page gives you access to tasks that are assigned to you and to members of your group. You can further filter the lists of tasks by due diligence requests, type of third-party action, and by risk or tiering assessment. See TPRM Task page.

List page

The List page is a general-purpose page that enables access to all items that you can view or act on in TPRM. See TPRM List page.

## Who can use the Vendor Management Workspace

The Vendor Management Workspace is designed for users with the following roles:

- TPR manager (Third-party risk manager) [sn_vdr_risk_asmt.vendor_risk_manager]
- TPR assessor (Third-party risk assessor) [sn_vdr_risk_asmt.vendor_assessor]
- Third-party assessment reviewer [sn_vdr_risk_asmt.vendor_assessment_reviewer]

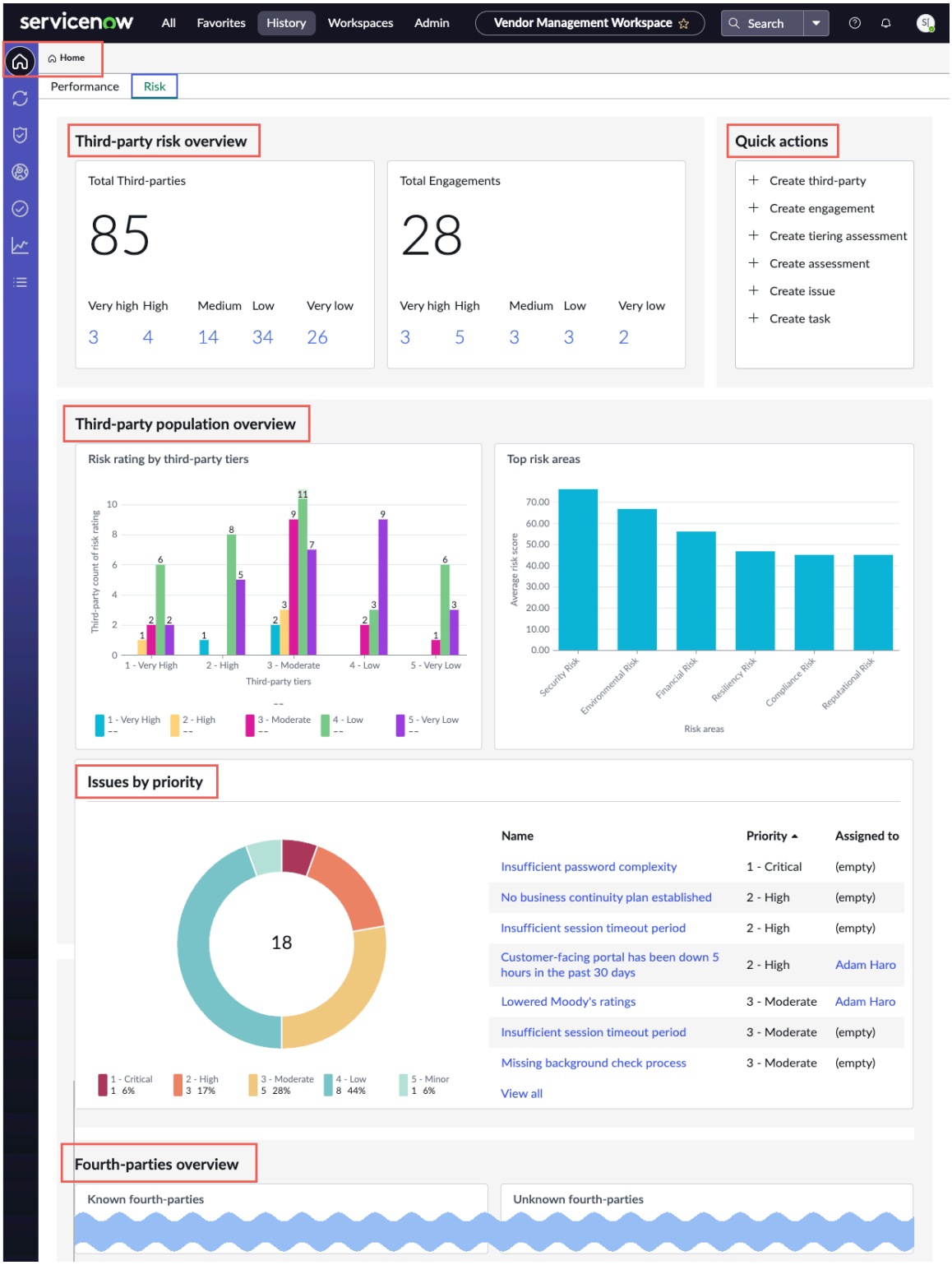
### TPRM Home page

The home page displays reports of important risk information and provides quick access to actions for TPR managers and TPR assessors.

## Accessing the page

To open the Home page on the Vendor Management workspace, select **Workspaces** > **Vendor Management Workspace**. Select and select the **Risk** tab.

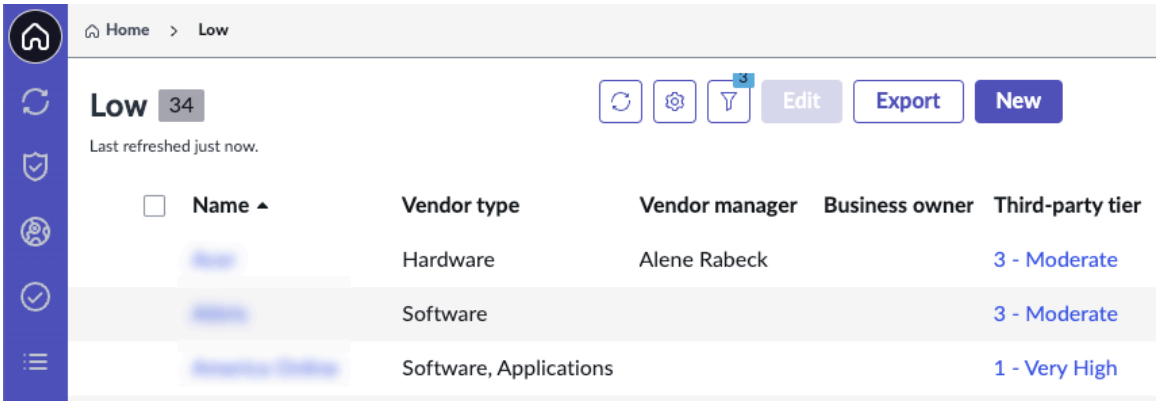
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




Third-party risk overview

Select any number in a box to open the associated list of third parties or engagements.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




After you open a list, you can select **Export** to export the data or select **New** to create a new engagement request.

Quick actions

- Create a third party record. Set up the key data and contact information for a third party that your organization will possibly engage. See Create a third party record—Legacy process.
- Define an engagement. Define an engagement so that you can assess the risks that are associated with the services or products offered by a third party. Engagements can also represent the products or services that are provided to the parent third party, either directly or from departments, partners, or subsidiaries that you can also assess for risk. Define an engagement — Legacy process.
- Create a tiering assessment. Organizations use risk tiering to classify their third parties into categories of potential risk posed at the time of onboarding. The standard predefined risk tiers are None, Low, Minor, Moderate, High, and Critical. Each risk tier has associated assessment questions and document requests. See Third-party risk tiering assessments — Legacy process.
- Create an assessment and initiate the third-party risk assessment life cycle. See Create an external risk assessment — Legacy process.
- Create an issue to help ensure that your concerns about a third party or engagement are remediated. See Create an issue for a third party or engagement.
- Create a task to help ensure that a user at your organization or the third-party contact responds to your concerns about questionnaire responses or requested documents during the due diligence process. See Create a task for a third party or engagement.

Third-party population overview

- **Risk rating by risk tiers**: The number of engagements at each risk rating for each third-party risk tier. See Set up risk rating scales and scoring.
- **Top risk areas**:

  The average risk score for engagements that are associated with each risk domain that you've defined.

  **Note:** Risk domains are called "risk areas" in some platform applications.

  A risk domain defines the type of risk to assess for a third party. For example, you might want to assess a data-management third party in terms of security

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

risk and a bank in terms of financial risk. Security risk and financial risk are risk domains. Some platform applications refer to risk domains as "risk areas." See Define a third-party risk domain.

Issues by priority

Count and priority of the highest priority open issues. Select an issue name to view the **Risk overview** tab of the issue page. See Manage issues.

Fourth-nth party overview

Counts of fourth parties and their sub-parties that are associated with third parties or engagements and unknown fourth parties.

### TPRM Due diligence management reports

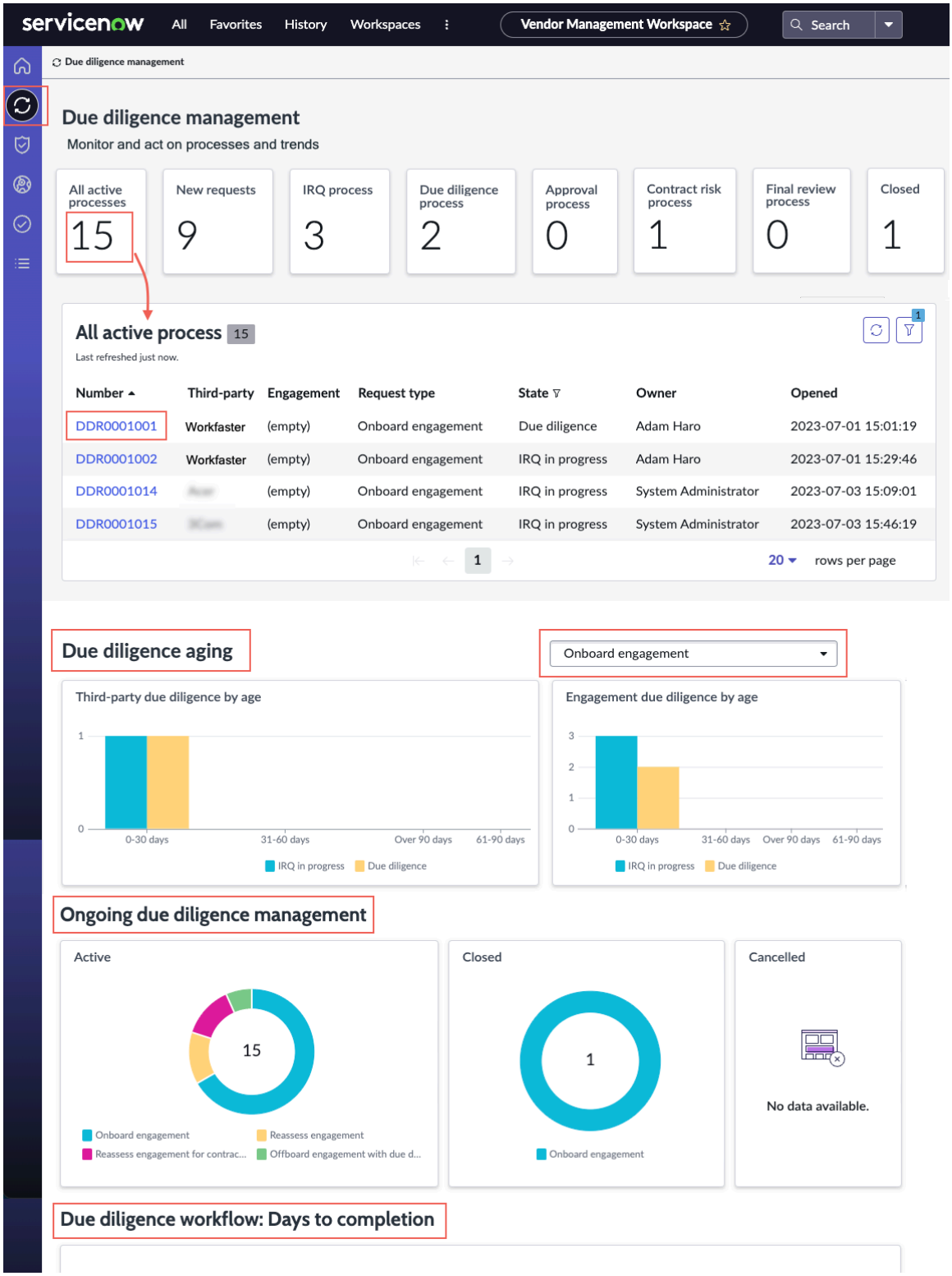
TPR managers and assessors use the due diligence management reports to track, prioritize, and manage their responsibilities.

## Accessing the reports

To view the due diligence management reports, select **Workspaces** > **Vendor Management Workspace**. On the **Risk** tab, select  .

**Tip:** TPR managers and TPR admins can perform a wide variety of tasks from the due diligence management dashboard. They can work on all processes in the workflow for a due diligence request: IRQs, external due diligence, approval, contract risk, and closed requests.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## Select items in the list view to work on engagement requests

By default, the page lists all active processes: IRQ, due diligence, approval, contract risk, and closed processes. Select the number on any card to view a list of actionable items for the process.

- Select the number on the **All active processes** card to view the list of active processes.
- Select the number on the **New requests** card to view the list of new requests.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Select the number on the **IRQ process** card to view the list of active IRQs. See IRQ process management for details.
- Select the number on the **Due diligence process** card to view the list of active third-party risk assessments. See Third-party (external) risk assessment management for details.
- Select the number on the **Approval process** card to view the list of requests in the approval process. See Managing the approval process for DD requests for details.
- Select the number on the **Contract risk process** card to view the list of requests in the contract process. See Managing the contract risk process for details.
- Select the number on the **Final review process** card to view the list of requests in the final review process.
- Select the number on the **Closed** card to view the list of closed requests for due diligence.

For each due diligence request, the system auto-assigns a unique ID number that starts with the text **DDR**. In any list, select the DDR number to view the request.

## Due diligence aging section

The Due diligence aging section displays the current duration of requests for due diligence for a third-party engagement: due diligence for third parties and for engagements. Use the list box to specify the type of due diligence request to display in the charts.

## Ongoing due diligence management

The Ongoing due diligence management section displays the current breakdown of **Active**, **Closed**, and **Cancelled** requests for due diligence.

## Due diligence workflow: Days to completion

The Due diligence workflow: Days to completion section displays the average completion time of each workflow over time.

Related topics

IRQ process management

Third-party (external) risk assessment management

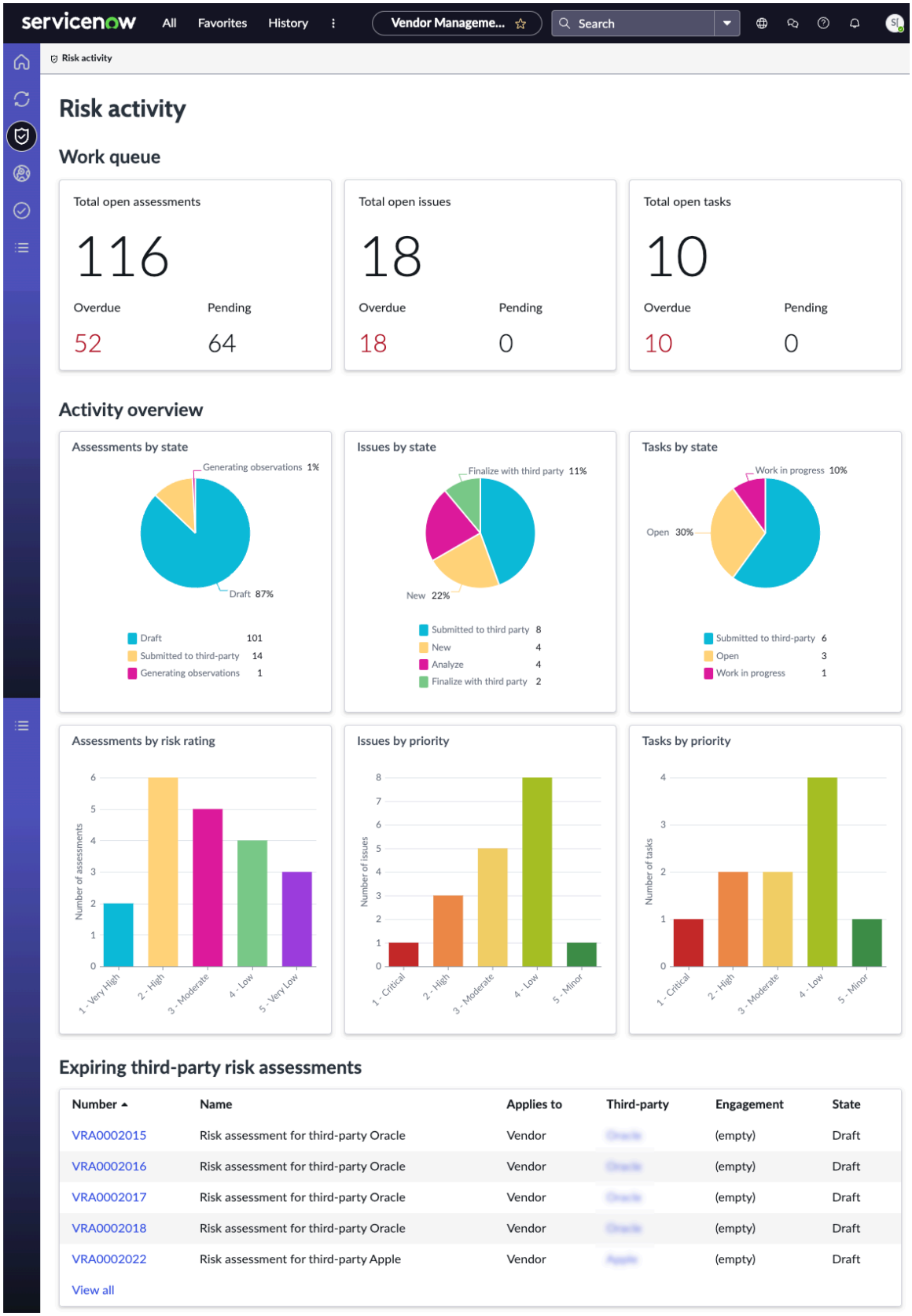
Managing the contract risk process

Managing the approval process for DD requests

### TPRM Risk activity page

The Risk activity page enables you to quickly identify assessments, issues, and tasks that need attention.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## Accessing the page

To view the Risk activity page, select **Workspaces** > **Vendor Management Workspace**. On the **Risk** tab, select .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Working on the page

Work queue

Select any number in a box to open the associated list of assessments, issues, or tasks.

Activity overview

Select any bar on a chart to open the associated list of assessments, issues, or tasks.

Expiring third-party risk assessments.

The section lists risk assessment due diligence requests that will expire soon.

For each external risk assessment, the system auto-assigns a unique ID number that starts with the text **VRA**. Select a VRA number to work on the risk assessment on the **Third-party risk assessments** tab.

### TPRM Risk concentration map

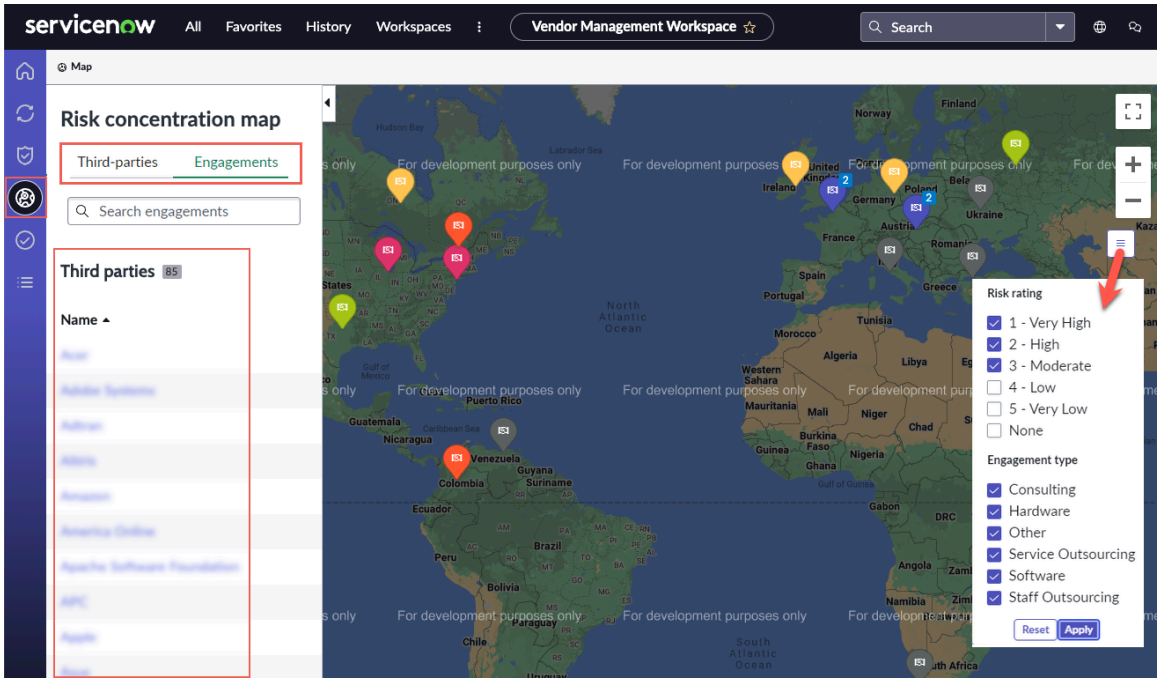
The Risk concentration map page pinpoints the geographical locations of active third parties and engagements. You can configure filters to view particular risk ratings and engagement types.

## Accessing the page

**Note:** This feature is available only if the Third-party Risk Management application has been activated. After you install the Risk concentration map feature, you must install a Google license to enable the feature. To enable the risk concentration map feature, see Enable the TPRM Risk concentration map.

- To view the Risk concentration map, select **Workspaces** > **Vendor Management Workspace**. On the **Risk** tab, select  .
- Because third-party locations might differ from engagement locations, the map enables you to view third-party locations separately from engagement locations. Select a tab to switch focus.
- Select the menu icon to open the list of filters that you can apply to the map.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

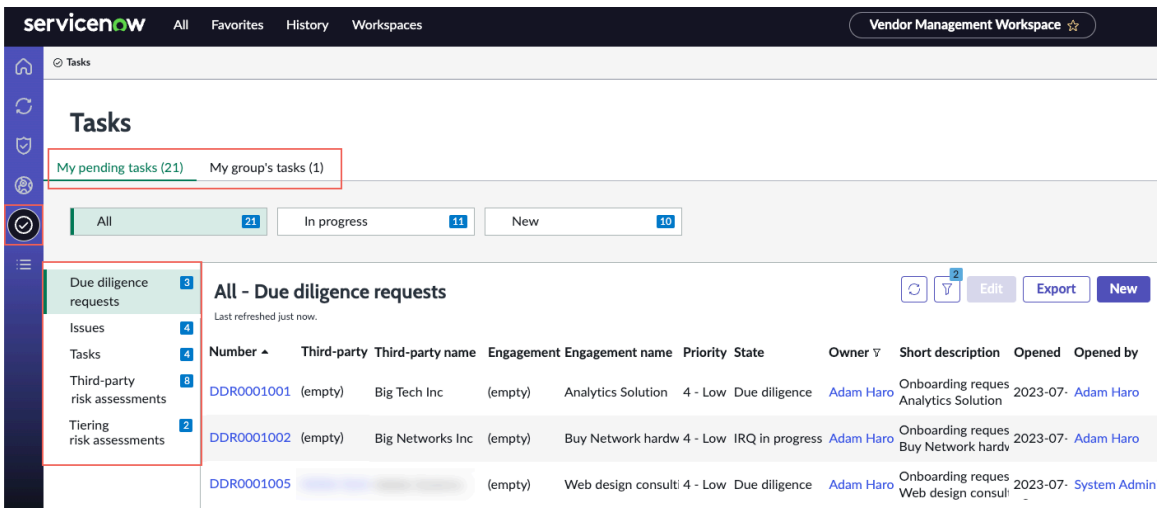



### TPRM Task page

The task page gives you access to tasks that are assigned to you and to members of your group. You can further filter the lists of tasks by due diligence requests, type of third-party action, and by risk or tiering assessment.

## Accessing the page

To view the Task page, select **Workspaces** > **Vendor Management Workspace**. On the **Risk** tab, select  .



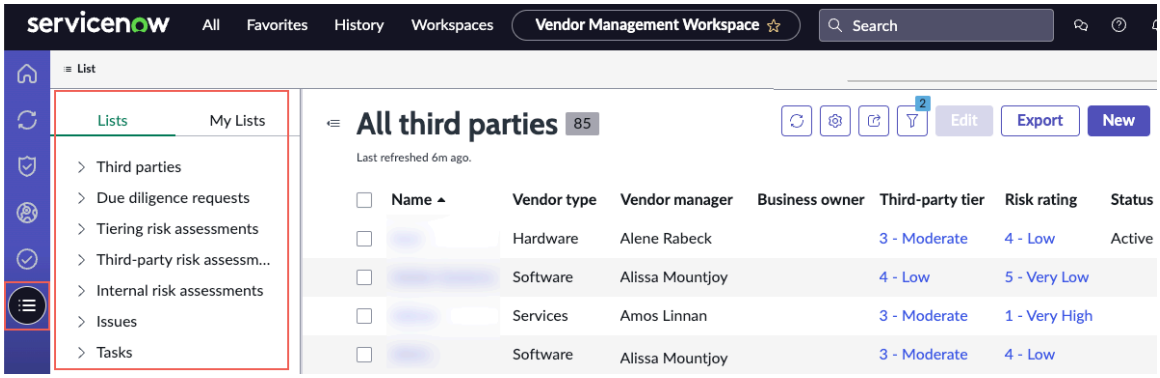

### TPRM List page

The List page is a general-purpose page that enables access to all items that you can view or act on in TPRM.

## Accessing the page

To open the List page, select **Workspaces** > **Vendor Management Workspace**. On the **Risk** tab, select the List icon  .

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

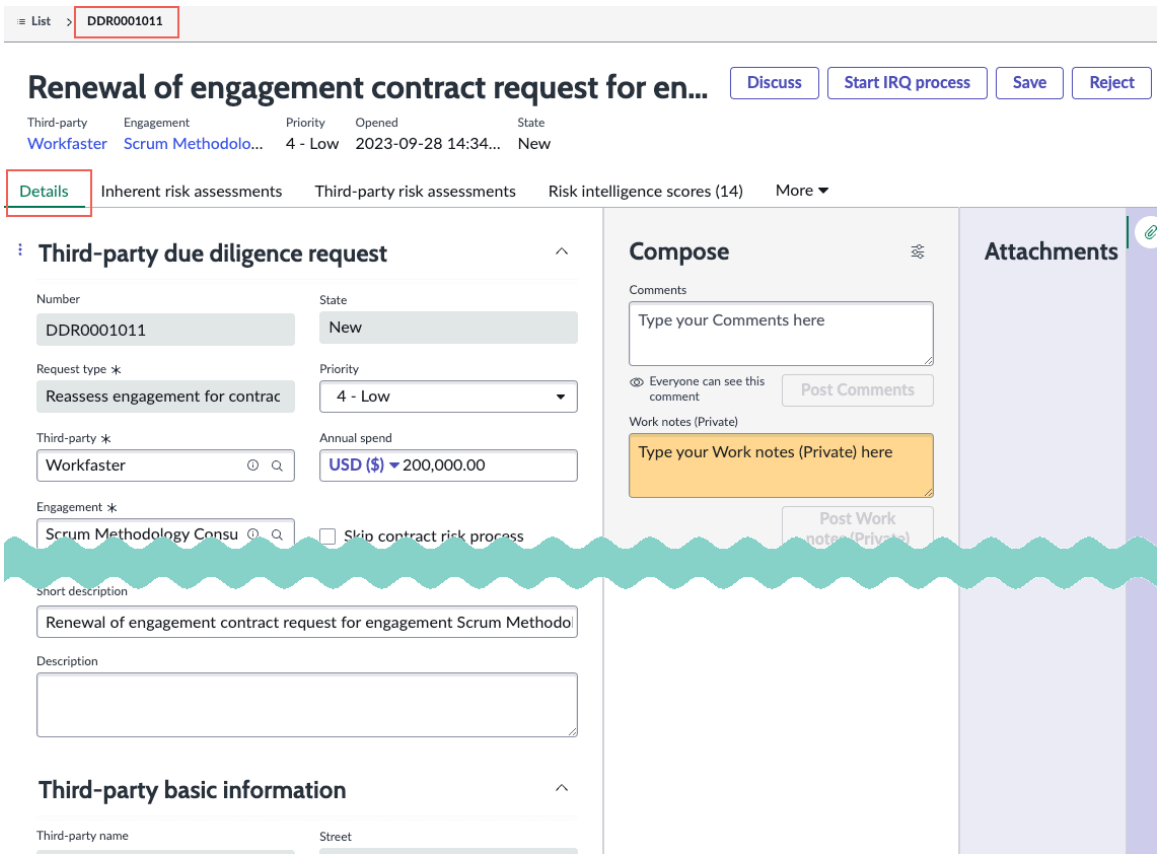



Each of the lists provides links to risk information and to action pages for your day-to-day tasks.

## Monitoring the due diligence request process

TPR managers and TPR admins can perform a wide variety of tasks from the due diligence management dashboard. They can work on all processes in the workflow for a due diligence request: IRQs, external due diligence, approval, contract risk, and closed requests.

For each due diligence request, the system auto-assigns a unique ID number that starts with the text **DDR**. You can access the Due diligence management page from many locations by selecting the **DDR** number for any due diligence request. The page opens to the **Details** tab. Typically, you start from the TPRM Home page.




## Monitoring processes from the request management page

Viewing basic information about a request on the Details tab

From the Details tab, you can view and adjust the due diligence request information. You can also log external-facing comments and private work notes,

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

attach files, and track request updates in the activity stream. See Due diligence request process management.

Monitoring the IRQ process

The first internal step after an engagement request is approved is to start the IRQ process to scope the risk by determining the third party's risk score. You can access the Due diligence management page from many locations by selecting the **DDR** number for any due diligence request. See IRQ process management.

Monitoring the external due diligence process (the third-party risk assessment process)

Select a VRA **Number** to open the Third-party risk assessments page in the Due diligence management page. See Third-party (external) risk assessment management.

Monitoring the approval process

You can view the list of users who can approve or reject a DD request and also view the details of their approval actions. In addition, you can view the approval levels for a request. See Managing the approval process for DD requests.

View the risk intelligence scores for a third party

The information on the **Risk intelligence scores** tab comes from risk intelligence provider services. Select any link to drill into the settings and scores. See Viewing risk intelligence scores.

Monitoring the Contract risk process

Protect your organization's interests, as the Third Party Risk contract negotiator, often the corporate counsel, by incorporating specific contractual provisions so that you can address the risks identified using the Third-party Risk Management application. See Accessing DD requests that are in the contract risk process.

## Actions on the Due diligence management pages

**Tip:** When you create (or the system generates) a new record (for example, a request for due diligence or a task), the system auto-assigns a unique ID number that helps to identify the type of data in the record. You can use the ID number to search for or filter the item you want to work on. See Unique ID numbers for TPRM records.

### Actions

| Action | Description |
|---|---|
| Start onboarding | For requests in the New state, this button enables the TPR manager to start the process. |
| Discuss | Select **Discuss** to send a message to other users. The message is recorded in the **Activity** section of the **Details** tab. |
| Save | Select **Save** to save any change you made to a value on any tab. |
| … Delete | Select **Delete** to delete the record of the engagement request. |
| Working in the Compose section | The **Compose section** on the **Details** tab enables you to permanently add text to the |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Actions (continued)**

| Action | Description |
|---|---|
| | record. The Activity section is updated with any actions on issues and tasks, submissions to TP contacts, and also with work notes and comments that users add to the record. Add text in the following fields as needed:<br>• **Work notes (Private)**: Information about the third-party risk assessment. Work notes are visible only to internal users who are assigned to the process.<br>• **Comments**: Comments about the third-party risk assessment are visible both to internal users and to third-party contacts. |
| Adding an attachment | Select **Browse** in the **Attachments** section to select and add an attachment. |

## Tracking a managed activity

View managed activities in the usage analytics activities table for tracking and verification purposes in the Third-party Risk Management application.

## Overview of managed activities

You can track and verify managed activities in the Usage analytics activities [sn_vdr_risk_asmt_ua_activity] table.

An engagement only consumes one license, regardless of whether there's one managed activity or many managed activities per contract year. Managed activity usage is triggered only when an activity is initiated.

Activities that are associated with a new third party going through the due diligence onboarding workflow aren't counted as managed activities. In this context, a new third party is defined as a company that is not in the Company [core_company] table.

If any of the following activities aren't related to a new third party going through the due diligence onboarding workflow, they're counted as managed activities:

- An Inherent risk questionnaire (IRQ) that is sent by the system has a status of **Awaiting response**. For more information, see Assessing your third-party risk.
- A tiering assessment with a questionnaire that is sent by the system has a status of **Awaiting response**. For more information, see Create and start a tiering assessment — Legacy process.
- A third-party risk assessment with a questionnaire that is sent by the system has a status of **Submitted to third party**). For more information, see Life cycle states of a third-party (external) risk assessment.
- The creation of a task or issue for a third-party risk assessment. For more information, see Create a task for a third party or engagement and Create an issue for a third party or engagement.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

If a third-party risk assessment or due diligence request is automatically created by an event-driven management rule and later recalled, it isn't counted as a managed activity. An assessment that is related to an event-driven management rule can be recalled up until the time that it's submitted to the third party. For more information, see Event-driven management — automate external assessment processes.

**Note:** If an assessment isn't related to an event-driven management rule, you can't recall it and it's counted as a managed activity. If an assessment is canceled, it's still considered as a managed activity.

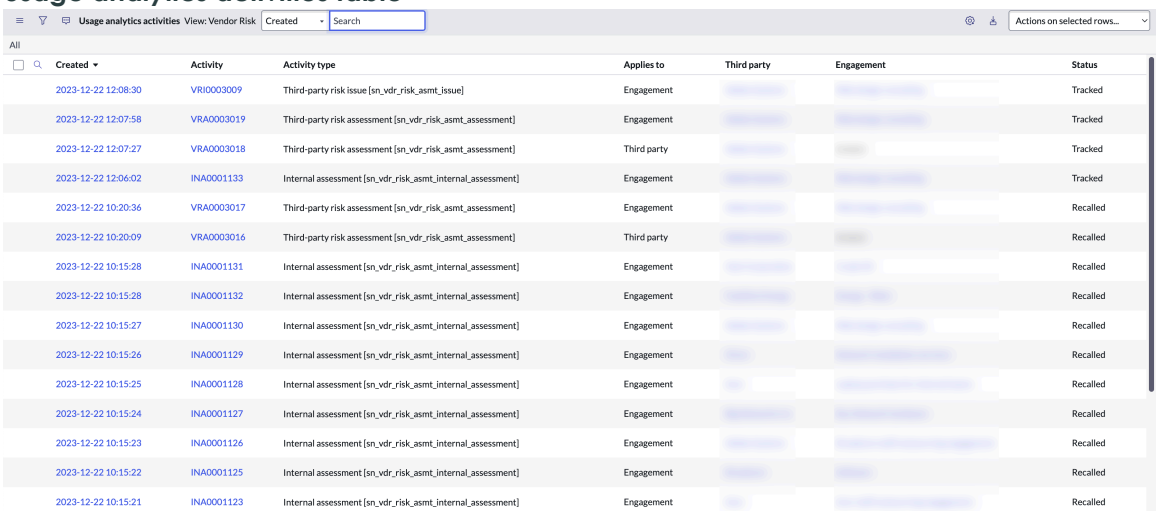
## Using the usage analytics activities table for verification

The usage analytics activities table stores a record every time a managed activity occurs. This table is read only. Records that are two years or older are automatically archived. You must have the Third-party assessment reviewer [sn_vdr_risk_asmt.vendor_assessment_reviewer] role to view this table.

You can access the Usage analytics activities table by navigating to **All** > **Third Party Risk Management** > **Administration** > **Managed Activity Analytics**.

The following example and table show the Usage analytics activities [sn_vdr_risk_asmt_ua_activity] table.

### Usage analytics activities table




### Usage analytics activities

| Field | Description |
|---|---|
| Created | Date and time that the activity occurred. |
| Activity | Record that is related to the activity. |
| Activity type | Managed activities that can be associated with tiering assessments, internal assessments, third-party risk assessments (TPRA), issues, and tasks. |
| Third party | Third party that is related to the activity. |
| Engagement | Engagement that is related to the activity. |
| Status | State of the activity: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Usage analytics activities (continued)**

| Field | Description |
|---|---|
| | • **Tracked**: The activity is logged.<br>• **Recalled**: The activity was recalled by a user after it occurred. |

**Note:** The calculated risk scores that are updated by assessments are managed activities. However, they aren't logged in the Usage analytics activities [sn_vdr_risk_asmt_ua_activity] table. The score updates from the risk intelligence score providers aren't managed activities. For more information on the risk intelligence scores, see Viewing risk intelligence scores.

## Approving or rejecting requests for due diligence

Use the Third-party Risk Management application to approve or reject new requests for due diligence, after reviewing questionnaire responses and due diligence process results.

### Approving due diligence requests

All internal stakeholders (approvers) review the external questionnaire responses and supporting documents that were provided by the third-party contact. You must be part of the Third-party risk (TPR) manager user group [sn_vdr_risk_asmt.vendor_risk_manager] to make approvals. Approvers perform all actions by using the Vendor Management Workspace or VRM Classic user interface. Approvers can view all of their pending **My approvals**, **Tasks**, and **Issues** by navigating to the Task page.

To view the Task page in the Vendor Management Workspace, select **Workspaces** > **Vendor Management Workspace**. Then, select the  .

To view your assigned approvals, select **My approvals**.

To view **My approvals** in the VRM Classic user interface, select **All** > **Self-Service** > **Third-party Risk Management** > **Due Diligence Requests** > **My Approvals**

From this view, you can accomplish the following tasks:

- Review the internal questionnaire responses.

  Navigate to the Due diligence request record page by selecting the **DDR** number and then selecting the **INA** number on the **Inherent risk assessment** tab. For more information, see IRQ process management.

- Review the risk intelligence scores.

  Navigate to the Due diligence request record page by selecting the **DDR** number and then selecting the **Risk intelligence scores** tab. For more information, see Viewing risk intelligence scores.

- Review the external questionnaire responses and supporting documents.

  Navigate to the Due diligence request record page by selecting the **DDR** number and then selecting the **VRA** number on the **Third-party risk assessment** tab. For more information, see Third-party (external) risk assessment management.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Access the approval request record page.

  Select one of the **Requested** states from the list to open the approval request record page. From this page, you can select **Approve** or **Reject**. For more information, see Managing the approval process for DD requests.

If the responses meet your requirements, one or more approvers approves the request and the owner (TPR manager or TPR assessor) closes the due diligence request and the engagement. The third party or engagement state is now **Active**. If a contract is going to be prepared, the approved due diligence request's state is updated to **Contract Risk Process** state.

For more information, see Managing the contract risk process.

**Note:** For information on how TPR admins can set approval levels and rules, see Set up the approval levels for due diligence requests and Set up the approval rules for due diligence requests.

## Rejecting due diligence requests

If an issue can't be resolved or the due diligence request is canceled, the approver can enter comments and reject the due diligence request. To view your **My approvals**, navigate to the task page, select **My approvals**, and then select a **Requested** state from the list to open the approval request record page. From this page, you can select **Reject** to reject the request.

After the due diligence request is rejected, the following actions occur:

1. The due-diligence request's state is updated from **Awaiting approval** to **Rejected**.
2. You must enter an explanation for rejecting the due diligence request in the **Comments** field.
3. The **Due diligence** process state is updated to **Rejected** and all stakeholders are notified that the engagement has been rejected.

**Note:** The owner can reopen the approval process by selecting the due diligence request from the All request list. The owner is required to provide justification for restarting the approval process.

## Managing the approval process for DD requests

You can view the list of users who can approve or reject a DD request and also view the details of their approval actions. In addition, you can view the approval levels for a request.

## Approval process

During the approval process, each aspect of risk is analyzed by the appropriate internal stakeholders. All internal stakeholders (approvers) review the questionnaire responses and supporting documents from the third-party contact. If the responses are good, one or more approvers approves and then closes the DD request. If a contract will be prepared, the approved request moves to the Contract Risk process.

## Accessing the Due diligence management page

You can access the Due diligence management page from many locations by selecting the **DDR** number for any DD request. Select either the **Approvers** tab or the **Approval levels** tab.

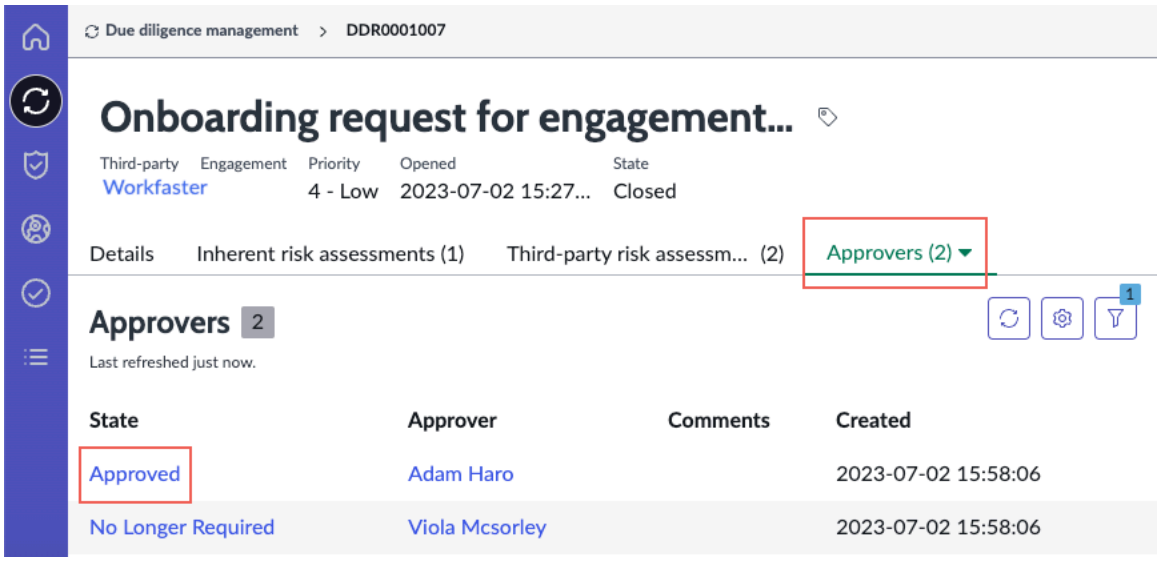
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Approvers tab

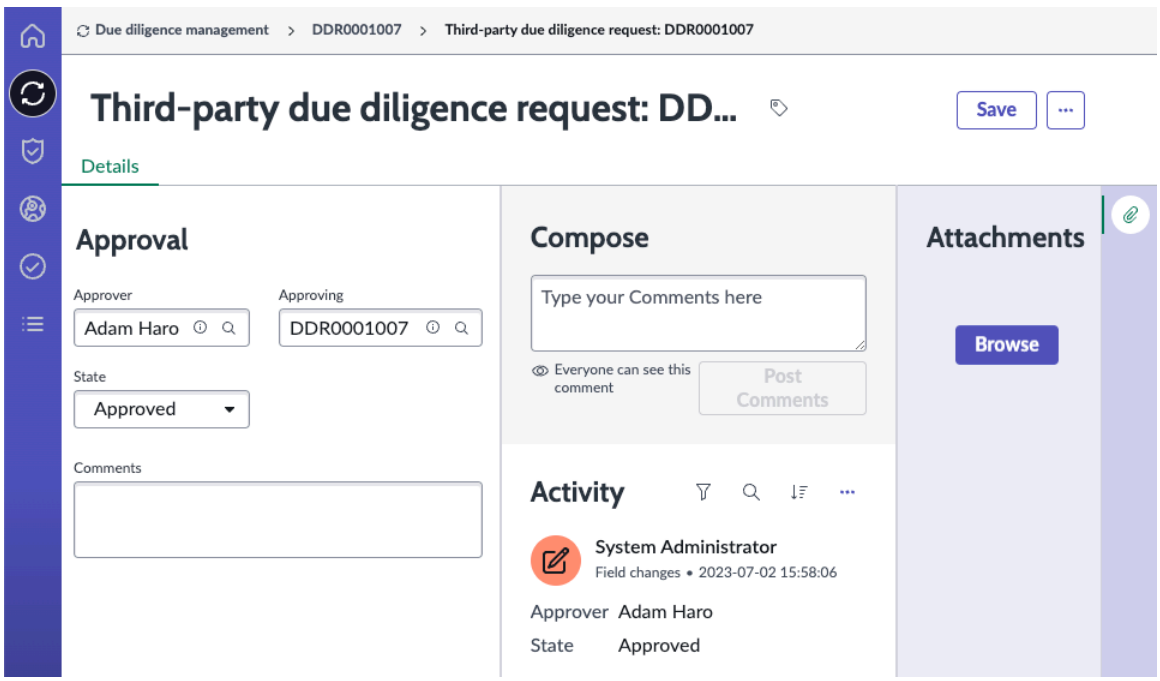
The tab lists the users that have responded to the engagement request. Select the **State** value to view the details of the approval action that the approver performed.

The state of the approval can be one of the following values:

- Not yet requested
- Requested
- Approved
- Rejected
- Cancelled
- No longer required

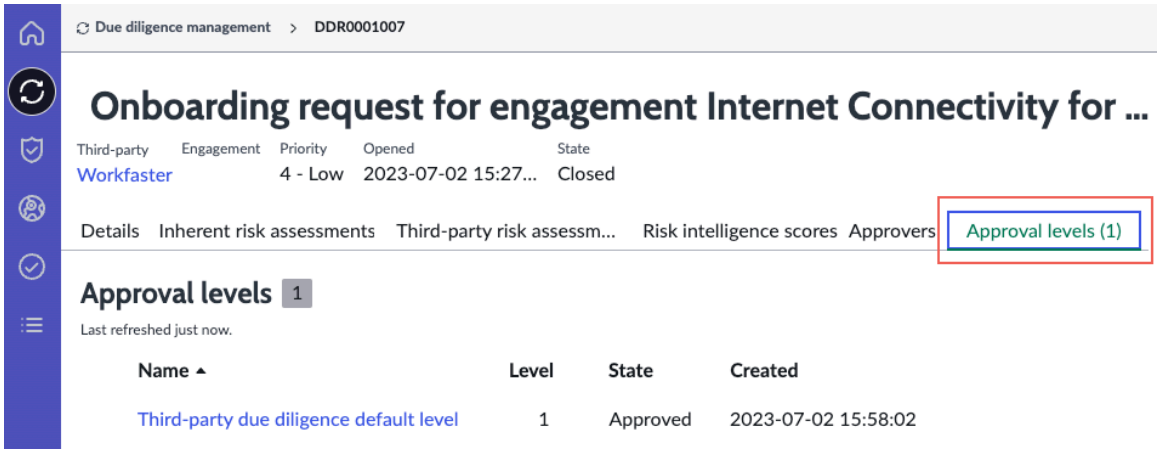



Select the **State** value for a request to view the **Details** tab for the request.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Approval levels tab




**Note:** For more information on how TPR admins can set approval levels and rules, see Set up the approval levels for due diligence requests and Set up the approval rules for due diligence requests.

Related topics

Create an issue for a third party or engagement

Create a task for a third party or engagement

## Managing the contract risk process

Protect your organization's interests, as the Third Party Risk contract negotiator, often the corporate counsel, by incorporating specific contractual provisions so that you can address the risks identified using the Third-party Risk Management application.

If a contract is being negotiated with the engagement or third party, the due diligence request enters the Contract risk process state after all approvals have been processed. If you're the assigned contract negotiator, you're notified through an automated email when all the approvals have been processed.

**Note:** The [sn_vdr_risk_asmt.contract_negotiator] role is required and your contract negotiator performs all actions by using the Vendor Management Workspace or VRM Classic user interface.

You can view all pending **Due diligence requests for Negotiator**, **Tasks**, and **Issues** by navigating to the Task page.

To view the Task page, select **Workspaces** > **Vendor Management Workspace**, and then select the task icon .

To view your assigned requests, select **Due diligence requests for Negotiator**.

To view **Due diligence requests for Negotiator** in the VRM Classic user interface, select **All** > **Self-Service** > **Third-party risk management** > **Due diligence requests** > **My Requests in Contract Process**

From this view, you can accomplish the following tasks:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Review the internal questionnaire responses.

  Navigate to the Due diligence request record page by selecting the **DDR** number. You can view the related internal questionnaire responses by selecting the **INA** number on the **Inherent risk assessment** tab. For more information, see IRQ process management.

- Review the risk intelligence scores.

  Navigate to the Due diligence request record page by selecting the **DDR** number. You can view the related risk intelligence scores by selecting the **Risk intelligence scores** tab. For more information, see Viewing risk intelligence scores.

- Review the external questionnaire responses and supporting documents.

  Navigate to the Due diligence request record page by selecting the **DDR** number. View the related external questionnaire responses and supporting documents by selecting the **VRA** number on the **Third-party risk assessment** tab. For more information, see Third-party (external) risk assessment management.

**Note:** To learn more about the processes in the due diligence workflow, see Due diligence workflow for more information.

Contract Risk process (Only if the engagement is contracted)

If the engagement includes a contract, as the contract negotiator, you prepare the contract and do the following actions:

1. Access all data that is generated during the Request, IRQ, Due Diligence, and Approval processes to design and settle the contract and assess the following items:
   - Initial Inherent Risk Questionnaire (IRQ) responses and comments by the Third-party risk assessor. For more information, see IRQ process management.
   - Risk data from the risk intelligence providers. For more information, see Viewing risk intelligence scores.
   - Responses to third-party questionnaires and engagement questionnaires. For more information, see Third-party (external) risk assessment management.
   - Issues and tasks for the third-party contacts that were assigned to you by the Third-party risk manager. Assigned issues and tasks are listed on the tasks page.
2. After the contract is fully signed by all parties (executed), attach the contract and activate the engagement by selecting **Contract executed** and then complete the following actions from the **Details** tab on the due diligence request record page:
   a. Set the **Contract start date** for the engagement. This date is read-only.
   b. Set the **Contract start date** for the third party if not set previously. This date is read-only.
   c. Set the **Contract expiration date** for the engagement to the requested end date. This date is read-only.
   d. Update the due diligence request's state from **Contract risk process** to **Engagement contract executed**.

**Note:** After opening an assigned task, select **Browse** in the **Attachments** section to select and add a contract.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Follow the same process in step 2 to activate an engagement for due diligence requests, onboard an engagement, and reassess an engagement for contract renewal.

Contract Risk process (contract is skipped)

If the engagement doesn't require a contract, you can skip the contract by selecting **Skip contract** from the **Details** tab on the due diligence request record page.

The following changes take place:

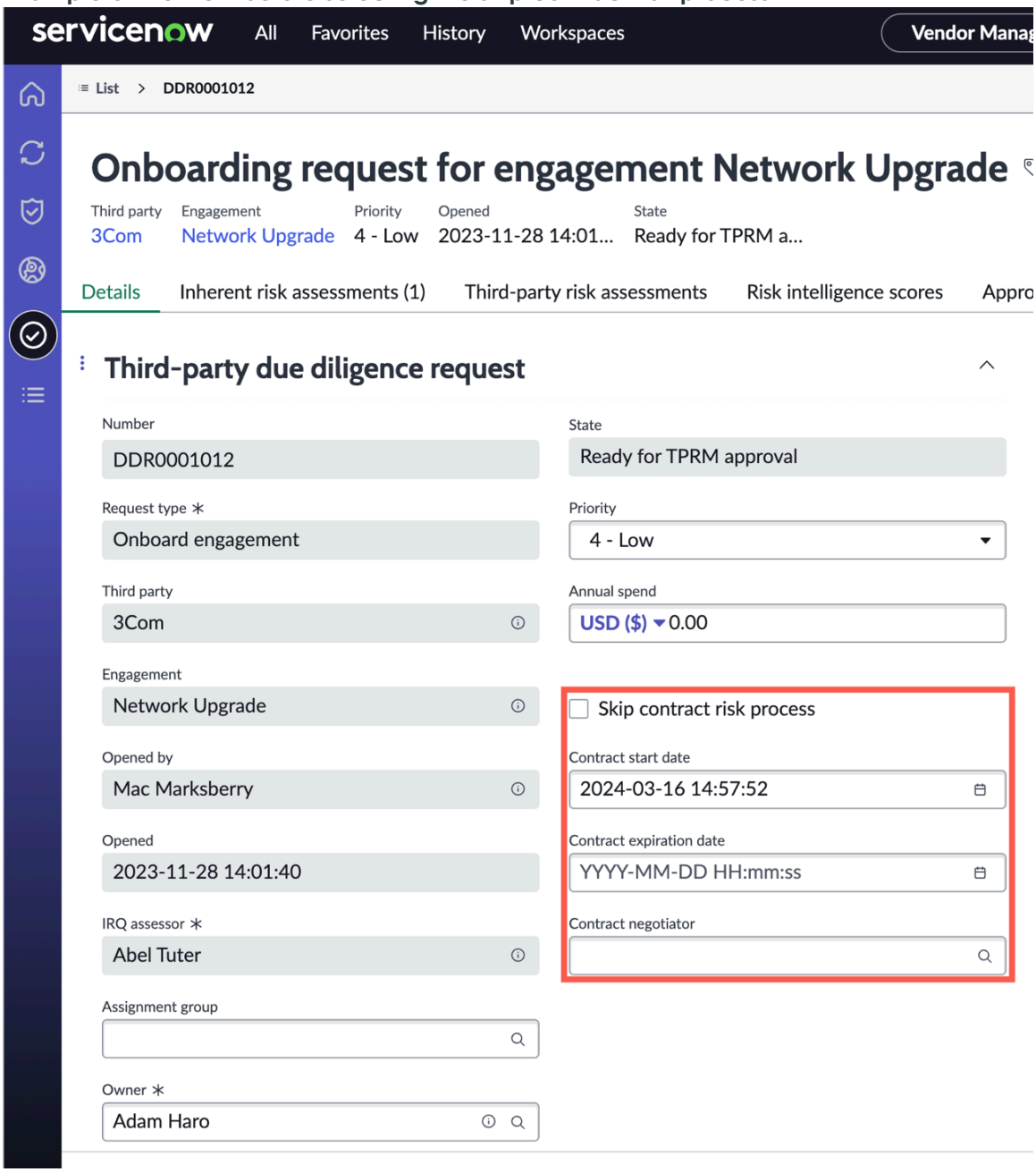
1. The **Contract start date** is changed to **Engagement start date**.
2. The **Contract end date** is changed to **Engagement expiration date**.
3. A required **Justification** field appears. Enter an explanation for skipping the contract.
4. The due diligence request's state is updated from **Contract risk process** to **Contract risk process skipped**.
5. After the owner closes the request, the engagement is **Active**.

**Note:** Skipping in this context is a way of intentionally not participating in the contract risk process that was initially scheduled or expected.

The following examples show the contract start and expiration date before and after you select the skip contract risk process.

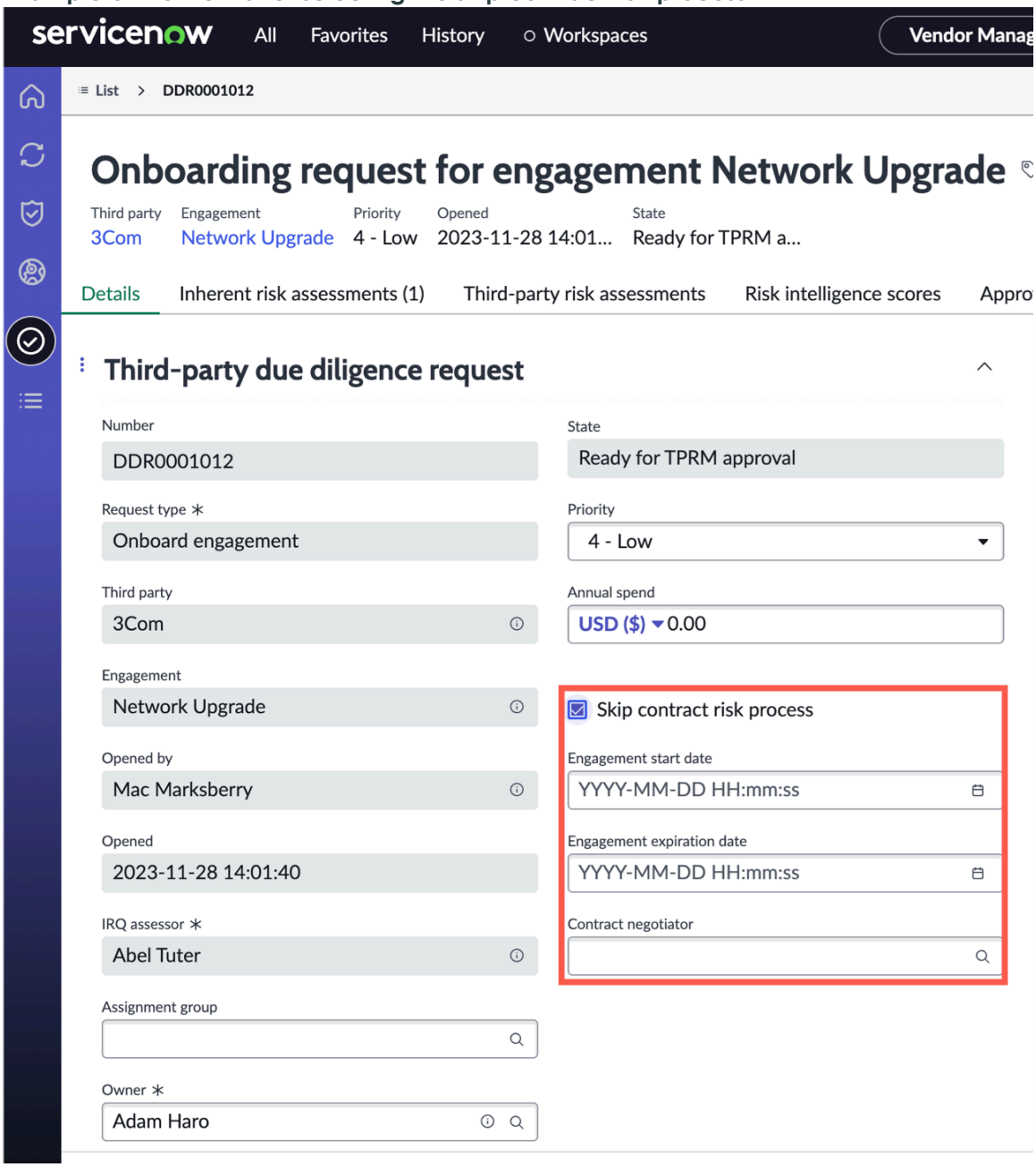
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Example of the view before selecting the skip contract risk process**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Example of the view after selecting the skip contract risk process**

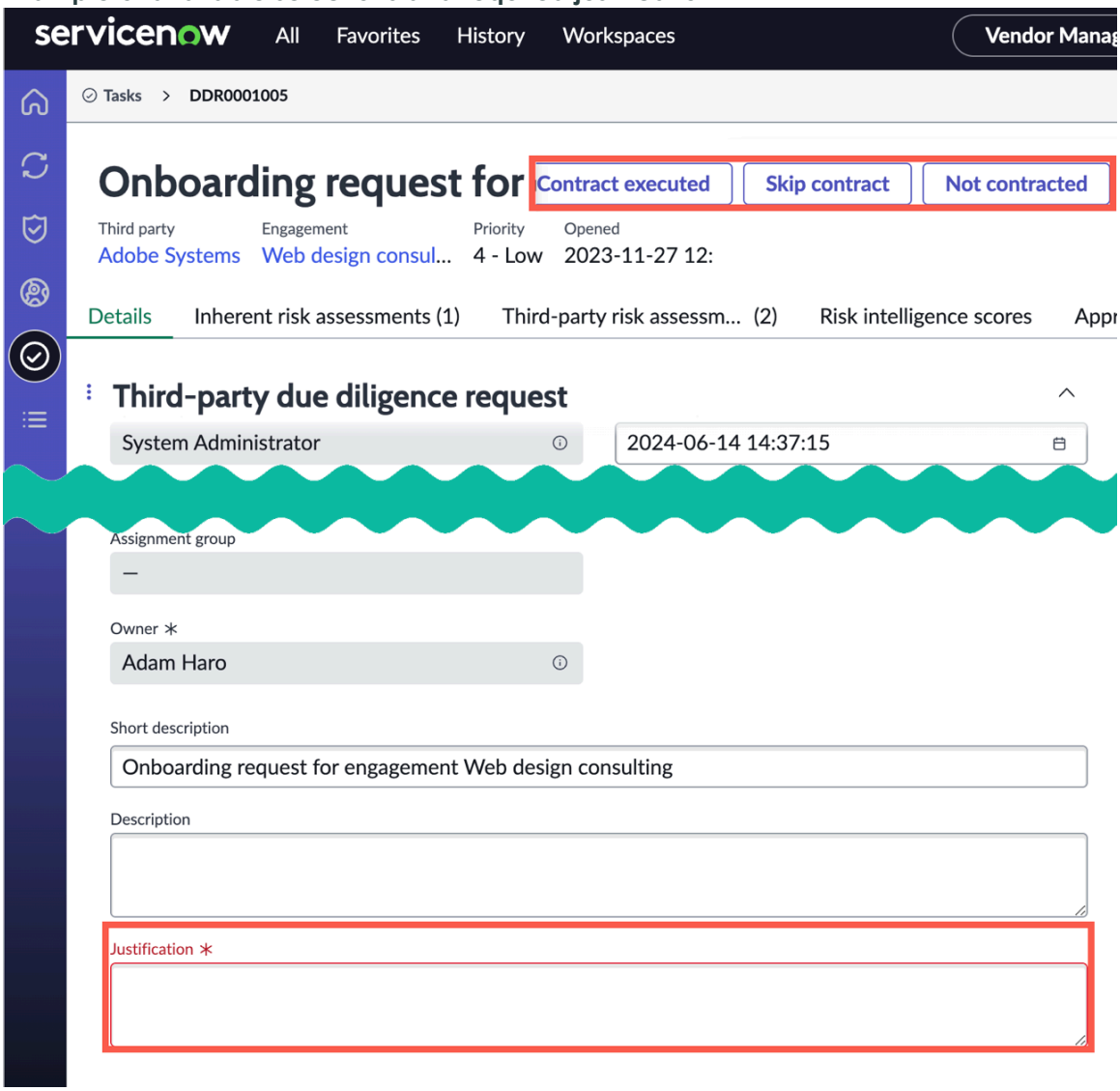



**Note:** If the third party risk manager or owner selects the **Skip contract risk process** option during the due diligence process, the assigned contract negotiator isn't notified and the **Contract risk process** state is skipped. An approver and owner can update the **Skip contract risk process** selection up until the approval process is completed. For more information about this process, see Due diligence request process management.

The following example shows the available selections and where the required justification box appears.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Example of available selections and required justification**




Contract Risk process (Not contracted, onboarding engagement is rejected)

If an issue can't be resolved or the due diligence request is canceled, you can reject the engagement by selecting **Not contracted** from the **Details** tab on the due diligence request record page.

The following actions take place:

1. A required **Justification** field appears. You must enter an explanation for rejecting the engagement.
2. The due diligence request's state is updated from **Contract risk process** to **Not contracted**.
3. After the owner closes the request, the due diligence request changes from **Not contracted** to **Rejected**.
4. All stakeholders are notified that the engagement isn't contracted and onboarding is rejected.

The owner can reopen the request and the due diligence request's state will update to the **Ready for TPRM approval** state.

Contract Risk process (Contract terminated)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

When the engagement is being offboarded and a contract is no longer required, you can approve the termination of the contract by selecting **Contract terminated**. The following actions then take place:

1. The due diligence request's state is updated from **Contract risk process** to **Contract terminated**.
2. The **Termination date** is updated with the current date.

Contract Risk process (Contract not terminated)

If the engagement is being offboarded (relationship terminated) and the contract can't be terminated, you can reject the request by selecting **Contract not terminated** from the **Details** tab on the due diligence request record page.

The following actions then take place:

1. A required **Justification** field appears. You must enter an explanation for rejecting the request.
2. The due diligence request's state is updated from **Contract risk process** to **Contract not terminated**.
3. After the owner closes the request, the engagement is **Rejected** and all stakeholders are notified that the contract isn't terminated.

Contract Risk process (Contract not renewed)

If the engagement is being reviewed for renewal and the contract can't be renewed, you can reject the engagement by selecting **Contract not renewed**.

The following actions then take place:

1. A required **Justification** field appears. You enter an explanation for rejecting the engagement.
2. The due diligence request's state is updated from **Contract risk process** to **Contract not renewed**.
3. After the owner closes the request, the engagement is **Rejected** and all stakeholders are notified that the contract isn't renewed.

Contract Risk process (Request additional due diligence)

If you require additional due diligence, you can reject the engagement by selecting **Request additional due diligence** from the **Details** tab on the due diligence request record page.

The following actions then take place:

1. A required **Justification** field appears. You must enter an explanation for requesting additional due diligence.
2. The due diligence request's state is updated from **Contract risk process** to **Due diligence**.
3. After the owner closes the request, it's updated to the **Due diligence** process state and all stakeholders are notified that the engagement requires additional due diligence.
4. Either you, as the contract negotiator, or the owner can reopen the assessment and attach a new questionnaire to restart the process.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

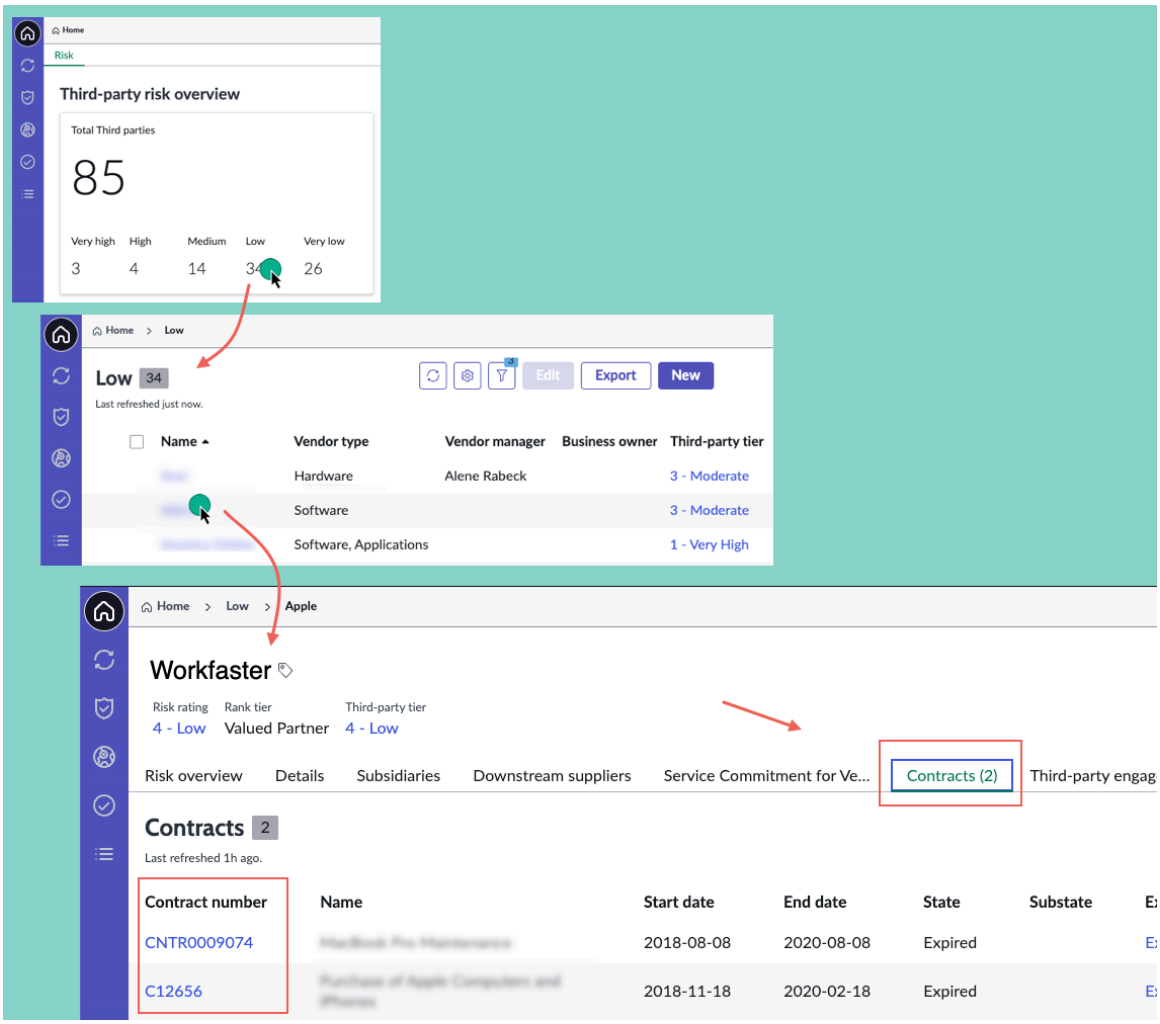
After the contract risk process is completed, the owner receives an email notification. Only the Third-party risk manager or owner can close a due diligence request.

## Accessing DD requests that are in the contract risk process

You can view the contracts associated with each engagement or third party and alongside detailed information such as expiration, start date, end date, and state. You can also manage and update contract processes.

## Accessing contract information

1. Select **Workspaces** > **Vendor Management Workspace**.
2. On the **Risk** tab, select the home page icon ( ).
3. In the Third-party risk overview section, select any number in a box to open the list of third parties or engagements with that value.
4. Select a third party or engagement name to open all tabs for the item and then select the **Contracts** tab.




5. Select a **Contract number** to view detailed information.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Viewing the list of contracts

### Contracts tab

| Column | Description |
|---|---|
| Contract Number | Assigned ID for the contract. The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Name | Brief description of the purpose of the contract. |
| Start date, End date | Dates for the beginning and end of interactions with the engagement. |
| State | Current state of the contract: Draft, Active, Expired, or Cancelled. |
| Substate | Current substate of the contract: Extension Active, Renewal Active, Awaiting Review, Under Review, Approved, Renewal Approved, Rejected, Renewal Rejected, Extension Approved, Extension Rejected. |
| Expiration | Current state of expiration: (empty), Expired, Within 30 days. |

## Actions on the contracts tab

### Actions

| Action | Description |
|---|---|
| New | Select **New** to create a contract. |
| Save | Select **Save** to save any change you made to a value on any tab. |
| … Delete | Select **Delete** to delete the record of the contract. |
| Adding an attachment | Select **Browse** in the **Attachments** section to select and add an attachment. |

## Managing processes from the contract page

Viewing basic information about a contract on the Details tab

From the details tab you can view and adjust contract information. You can also attach files.

Viewing child contracts

View all contracts that have the current contract as a parent. Select a CNTR **Number** to open the child contract page.

Managing the contract

See Contract Management.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Working in the VRM Classic user interface

While you can continue to use the legacy user interface to perform Vendor Risk Management tasks, the Vendor Management Workspace offers enhanced TPRM features and more useful reports.

## Configure risk assessment to recur on a schedule

Configure a third-party risk assessment to recur on a schedule to regularly update risk results for a third party or an engagement.

Role required: sn_vdr_risk_asmt.vendor_assessor

## Create a third party record—Legacy process

Configure a third-party risk assessment to recur on a schedule to regularly update risk results for a third party or an engagement.

Role required: admin or sn_vdr_risk_asmt.vendor_risk_manager.

## Setting up third-party hierarchies and engagements—Legacy process

Create third-party hierarchies by defining the parent-child relationships between the parent third party and all of their subsidiaries. You do this task because some organizations work with third parties that have subsidiaries (or subsidiaries of subsidiaries) that can pose a potential risk to your business. You can perform assessments at each subsidiary organization and roll up the results to calculate an overall risk score for the parent third party.

Role required: sn_vdr_risk_asmt.vendor_risk_manager or sn_vdr_risk_asmt.vendor_assessor.

## Define an engagement — Legacy process

Define an engagement so that you can assess the risks that are associated with the services or products offered by a third party. Engagements can also represent the products or services that are provided to the parent third party, either directly or from departments, partners, or subsidiaries that you can also assess for risk.

**Tip:** Any person with access to your instance at your organization can request an engagement. That process is typically more streamlined and more effective than the process describe here, where a Third-party risk (TPR) manager or TPR assessor defines an engagement. For more information, see Request due diligence for a third-party engagement.

Role required: sn_vdr_risk_asmt.vendor_risk_manager or sn_vdr_risk_asmt.vendor_assessor.

## Third-party risk tiering assessments — Legacy process

Organizations use risk tiering to classify their third parties into categories of potential risk posed at the time of onboarding. The standard predefined risk tiers are None, Low, Minor, Moderate, High, and Critical. Each risk tier has associated assessment questions and document requests.

## Managing external risk assessments — Legacy process

Before the TPR manager closes an assessment, stakeholders create issues and tasks, usually during the **Generating observations** state. The TPR assessor assigns third parties as needed and communicates using comment streams to achieve closure on non-compliance. The third-party primary contact uses the Third-party portal to view all assessments.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Create an external risk assessment — Legacy process

Create an assessment and initiate the third-party risk assessment life cycle.

## Configure risk assessment to recur on a schedule

Configure a third-party risk assessment to recur on a schedule to regularly update risk results for a third party or an engagement.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_assessor

### Procedure

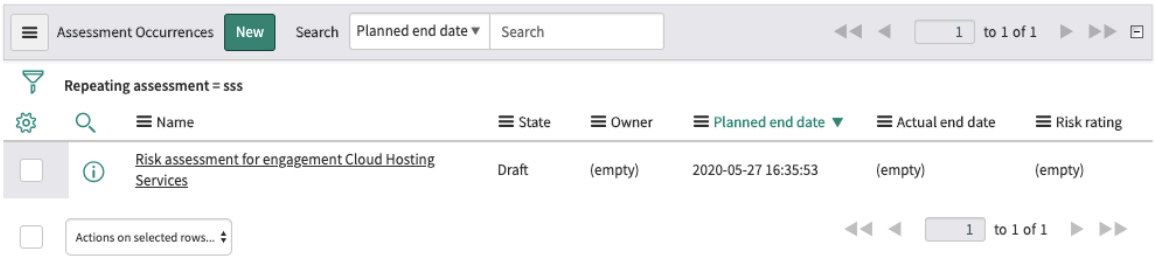
1. Navigate to **All** > **Third-party Risk Management** > **External Risk Assessments** > **Repeating Assessments**.
2. Click **New**, fill in the form, and then click **Submit**.

**Repeating Assessment form**

| Field | Description |
|---|---|
| Number | For each external risk assessment, the system auto-assigns a unique ID number that starts with the text **VRA**.<br><br>The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Description | Detailed description of the recurring assessment. |
| Name | Name of the recurring assessment. |
| Assessment template | Template used to create the current assessment. |
| Applies to | The entity to which the assessment applies: **Vendor** or **Engagement**. |
| Vendor | Vendor that is being assessed. |
| Engagement | Select the engagement being assessed.<br><br>The field is visible only if you selected **Engagement** in the **Applies to** field. |
| Active | Option to enable the current recurring assessment to run when scheduled. |
| Next assessment creation (months) | The next assessment will be created in the specified number of months after the previous assessment is closed. |
| Next assessment end date (months) | The end date for the new assessment after the previous assessment is closed. |
| Assessment results valid duration (days) | The number of days that the assessment results are valid. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **Assessment occurrences** related list displays the status of each time the assessment took place and the risk rating that resulted from the assessment.




## Create a third party record—Legacy process

Set up the key data and contact information for a third party that your organization will engage.

### Before you begin

Contact your system administrator before you update the portfolio of third parties.
Role required: sn_vdr_risk_asmt.vendor_risk_manager or sn_vdr_risk_asmt.vendor_risk_admin

### About this task

In addition to adding new records, TPR managers make ongoing updates to third-party information, including risk security scores, risk tiers, critical third-party contacts, and the business services that the third parties fulfill.

You can import third-party data from a spreadsheet, integrate the data from an onboarding system, or import data from the vendor table.

### Procedure

1. Use either of the following methods to start the process:
   - In the Vendor Management Workspace, click the List icon ( ) and then navigate to **Third parties** > **All Third parties**.
   - Navigate to **All** > **Third-party Risk Management** > **All Third parties**.
2. Click **New** and then fill in the fields.

#### Third party form

| Field | Description |
|---|---|
| Name | Third party name. |
| Website | URL for the third party. |
| DUNS number | Unique numeric identifier for the single business entity. A DUNS number is not legally required for a business. |
| Industry | Type of industry. |
| Vendor type | Specify the type of product or service that the third party will provide. |
| Parent | If you set up third-party hierarchies, and this third party is a subsidiary, select the parent third party. |
| Total annual spend | Expected amount that you expect to spend annually on this third party. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Security Score | The security score provided by a risk intelligence provider. |
| Score provider | The risk intelligence provider that provided the normalized security score. |
| Status | Status of the third party. |
| Contract start date | Date that the contracted engagement should start. |
| Risk rating | After third-party risk assessment responses have been received, this weighted average of the components (that is, the risk ratings of assessments, engagements, and subsidiaries) is calculated. For more information, see Setting up third-party hierarchies and engagements—Legacy process. |
| Rank tier | Type of supplier. |
| Third-party tier | Risk tier for the third party calculated by mapping the tiering score to a risk tier. |
| Vendor manager | The employee assigned as the manager to this third party. |
| Business owner | The employees that use this third party in their daily business. |
| Notes | Additional information. |
| **Contact tab** | |
| Street | Street address of third party. |
| City | City of third party. |
| State / Province | State or Province of the third party. |
| Zip / Postal code | Zip code or postal code of the third party. |
| Country | Country of the third party. |
| Phone | Phone number of the third party. |
| Fax phone | Fax number of the third party. |
| **Profile tab** | |
| Publicly traded | Is the third party publicly traded? |
| Stock symbol | Stock symbol of the third party. |
| Revenue per year | Annual revenue of the third party. |
| Number of employees | Count of the third party's employees. |
| Banner image | Banner image for the third party. |
| Banner text | Banner text for the third party. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| **Risk Scoring tab** | |
| Computed risk rating | Average of the third-party risk area risk ratings. |
| Override risk rating | Enables you to override the computer risk rating for the third party. |
| Assessment risk rating | Calculated risk assessment rating. The risk rating scale helps business users better understand risk assessment results. For example, in the default settings, risk scores in the 20 through 39 range indicate high risk, while scores in the 60 through 79 range indicate low risk. |
| Engagement risk rating | Calculated engagement rating. The risk rating scale helps business users better understand risk assessment results. For example, in the default settings, risk scores in the 20 through 39 range indicate high risk, while scores in the 60 through 79 range indicate low risk. |
| Subsidiary risk rating<br><br>Child third-party risk rating | Calculated risk rating for subsidiaries. The risk rating scale helps business users better understand risk assessment results. For example, in the default settings, risk scores in the 20 through 39 range indicate high risk, while scores in the 60 through 79 range indicate low risk. |
| Risk intelligence rating | See Integrating scores from risk intelligence providers. |
| Overridden risk rating | If you selected **Override risk rating**, enter the new risk rating. |
| Overridden on | If you selected **Override risk rating**,date that the override occurred. |
| Justification | If you selected **Override risk rating**, you must enter a reason for the override. |

3. If Third-party Risk Management is integrated with other GRC applications, or if you set up vendor hierarchies (that is, third-party risk domains, component criteria, and risk scoring rules), the form can include some or all of the following related lists.

   For more information, see Setting up third-party hierarchies and engagements—Legacy process.

   **Note:** Risk domains are called "risk areas" in some platform applications.

   - **Child Vendors:** This table stores all information for subsidiaries. Subsidiary risk ratings are automatically aggregated and displayed on the **Risk Rating** tab on the Third-party form.
   - **Vendor Contacts:** This table stores information for all of the third-party stakeholders. Typically, the customer creates one primary third-party contact and one or more secondary contacts. The primary contact adds other contacts to the list.
   - **Business Services:** The Services table is part of the CMDB. It relates the third parties to the services they provide. For example, assume the IT team has a service called “Video

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Conference Services" that is used for internal employees to communicate internally and with customers. That business service, they have decided, comes from Zoom rather than building anything in-house.

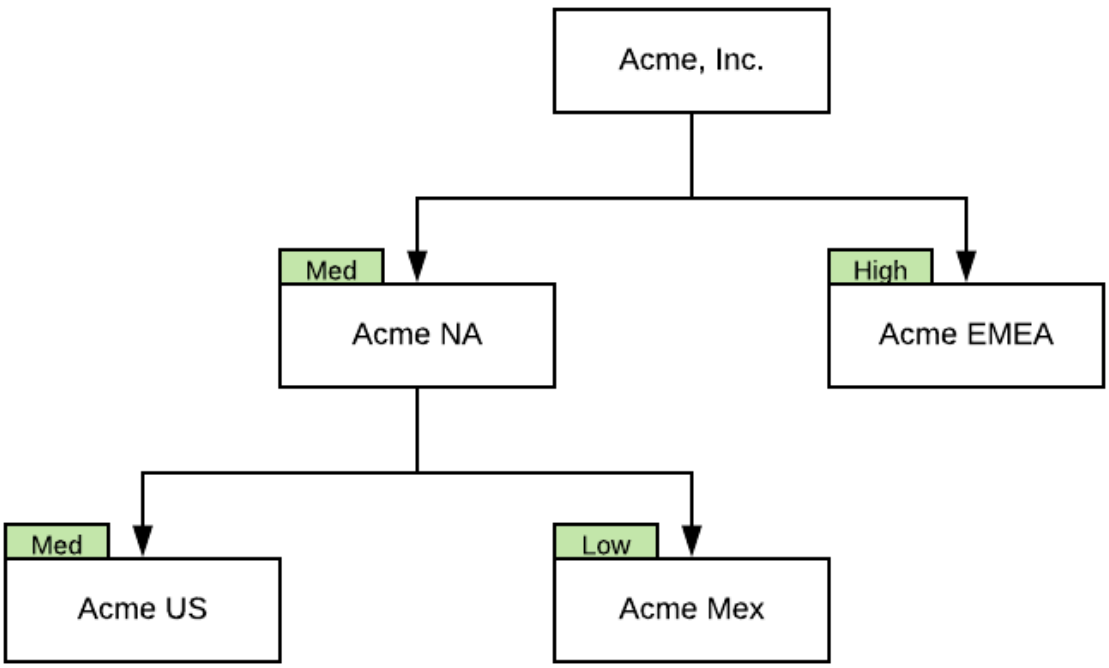
- **Vendor Engagements:** This table stores all engagement information for third parties. Engagements risk ratings are automatically aggregated as displayed on the **Risk rating** tab on the Third-party form.
- **Tiering Assessments:** This table stores the history of tiering assessments.
- **Repeating Assessments:** This table stores the history of recurring assessments.
- **Assessments:** This table stores the history of assessments. Assessment risk ratings are automatically aggregated and displayed on the **Risk rating** tab on the Third-party form.
- **Vendor Risk Components:** This table stores all third-party risk components. If third-party risk components (that is, assessments, engagements, or subsidiaries) are present, their risk ratings are automatically aggregated and displayed on the **Risk rating** tab on the Third-party form.
- **Issues:** This table stores the history of issues.
- **Tasks:** This table stores the history of tasks.

## Setting up third-party hierarchies and engagements—Legacy process

Create third-party hierarchies by defining the parent-child relationships between the parent third party and all of their subsidiaries. You do this task because some organizations work with third parties that have subsidiaries (or subsidiaries of subsidiaries) that can pose a potential risk to your business. You can perform assessments at each subsidiary organization and roll up the results to calculate an overall risk score for the parent third party.

### Third-party hierarchy

In this example, parent organization Acme has two subsidiaries and Acme NA has two subsidiaries. In this hierarchy, you perform risk assessments for the parent third party and all subsidiaries and calculate risk scores for each entity. You can then aggregate (roll up) the risk scores to calculate the risk score for Acme.

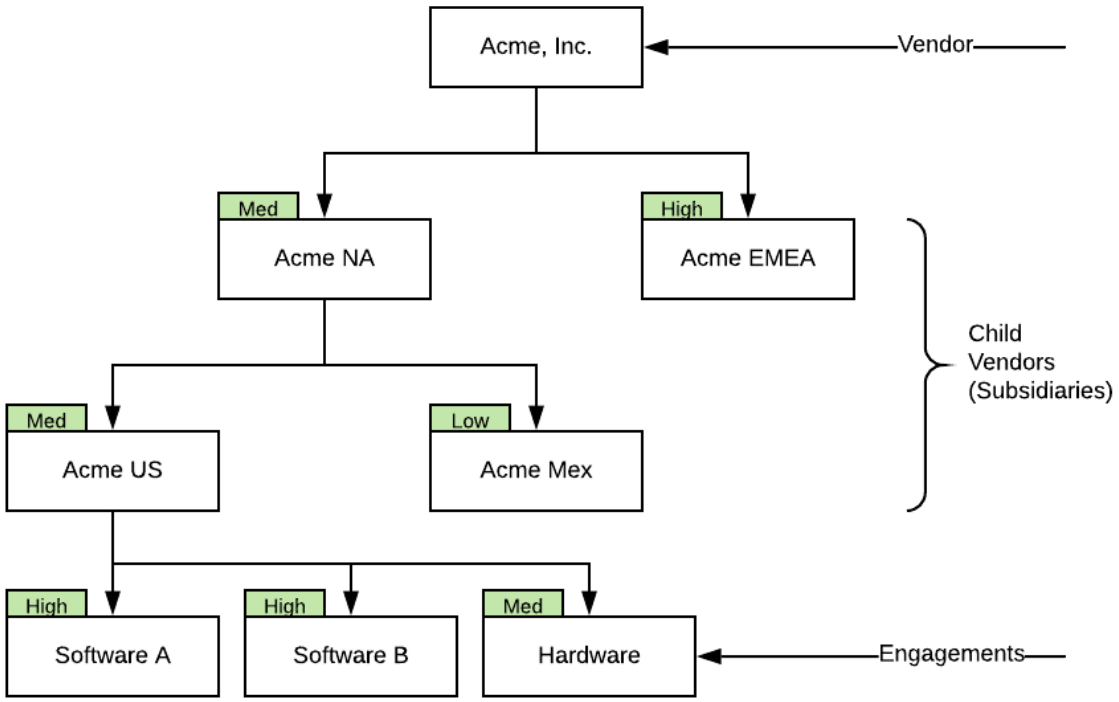



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Third-party hierarchy with subsidiaries and engagements

Engagements represent products or services provided to the parent organization—either directly or from subsidiaries—that you can assess for risk. In the case where a subsidiary provides engagements, the risk scores assigned to the engagements are rolled up to calculate the risk score of the subsidiary, which in turn roll up to the parent organization.

In this example, subsidiary Acme US has three engagements. As in the previous example, risk is assessed for the parent, all of its subsidiaries, and all of their engagements. The risk scores are then rolled up to calculate the risk score for the parent.




See Define an engagement — Legacy process.

## Overview: Setting up a third-party hierarchy

**Note:** The setup procedures in this section apply only if you work with multi-layered third parties; that is, third-parties that operate subsidiaries. They also guide you through the setup of engagements offered by subsidiaries. If these are not the types of third parties you do business with, and you do not want to set up third-party hierarchies, these procedures are optional.

### Setup procedures for third-party hierarchies

| Setup procedure | Description |
|---|---|
| Define third-party risk areas. | A risk domain defines the type of risk to assess for a third party. For example, you might want to assess a data-management third party in terms of security risk and a bank in terms of financial risk. Security risk and financial risk are risk domains. Some platform applications refer to risk domains as "risk areas."<br><br>See Define a third-party risk domain. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Setup procedures for third-party hierarchies (continued)**

| Setup procedure | Description |
|---|---|
| Define third-party risk area criteria. | A third-party risk area criteria is a group of risk domains (sometimes called risk areas in other platform features) that applies to a particular type of third party.<br><br>See Define third-party risk area criteria. |
| Define component criteria. | Components are the entities for which you can assess risk. The base system includes the engagements, external monitoring, subsidiaries, and third-party risk assessments components. Risk is calculated for each component and then the risk is aggregated and rolled up to calculate a third-party risk rating.<br><br>See Define component criteria. |
| Define engagements for a third party | Define an engagement so that you can assess the risks that are associated with the services or products offered by a third party. Engagements can also represent the products or services that are provided to the parent third party, either directly or from departments, partners, or subsidiaries that you can also assess for risk.<br><br>As engagements are defined, you can define primary and secondary contacts for both third parties and engagements. Each type of contact can perform specific activities in the Third-party portal.<br><br>See Define an engagement — Legacy process. |
| Define engagement risk scoring rules. | An engagement risk-scoring rule specifies component criteria that determine which engagements are selected for assessment. For example, a rule could enable assessments for engagements that involve more than $40,000 annual business. Engagement scoring rules apply only to engagements.<br><br>See Define engagement risk scoring rules. |
| Define third-party risk scoring rules. | Define criteria, based on risk scores, that determine which third parties require assessments. Third-party risk scoring rules apply to subsidiaries and engagements and to third-party risk areas.<br><br>See Define third-party risk scoring rules. |

## Define an engagement — Legacy process

Define an engagement so that you can assess the risks that are associated with the services or products offered by a third party. Engagements can also represent the products or

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

services that are provided to the parent third party, either directly or from departments, partners, or subsidiaries that you can also assess for risk.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager or sn_vdr_risk_asmt.vendor_assessor

### Procedure

1. On the **Risk** tab of the Vendor Management Workspace, select **Create engagement** in the Quick actions box.
   The Create third-party engagement form opens to the **Details** tab.
2. Optional: Click **Browse** to select and add an attachment.
3. Fill in the form an then click **Save**.

**Create third-party engagement form**

| Field | Description |
|---|---|
| **Third-party engagement section** | |
| Name | Unique name for the engagement. Ideally, mention the product or service that is the subject of the engagement. |
| Third party (Vendor) | The third party for whom you are creating this engagement record. |
| Type | Type of product or service to be provided by the engagement organization. |
| Start/End date | Enter start and end dates to define how long the engagement is valid. |
| Contract start date / end date | Preferred dates for the beginning and end of interactions with the third party. |
| Contract expiration date | The date on which the engagement ends officially and legally. |
| Status | Select the current status of the engagement.<br>◦ Active<br>◦ Onboarding<br>◦ Prospect<br>◦ Active unauthorized<br>◦ Terminated<br>◦ Onboarding rejected<br>**Note:** An engagement starts in the inactive state. An engagement moves to the active state when a contract is in place or you take part in an active relationship with the third party. |
| Risk rating | Displays the risk rating assigned to the engagement after an assessment has been performed. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Engagement tier | The tier used for this engagement. See Third-party risk tiering assessments — Legacy process for details of how the tier is determined. |
| Annual spend / Value | The annual monetary spend associated with this engagement's services. |
| Engagement manager | Specify the person who will monitor, prioritize, and act on responses to external questionnaires, issues, and tasks. Click the lock to lock/unlock the field. |
| Business owner | Specify the person who is familiar with the engagement organization and the product or services that will be engaged. Click the lock to lock/unlock the field. |
| Notes | Enter text that describe the engagement to other users. |
| **Contact section** | |
| Street, City, State/ Province, ZIP/Postal code, Country, Phone, Fax | Standard contact information for the engagement organization. |
| Latitude and Longitude | The **Latitude** and **Longitude** values are used to mark the location on the Risk concentration map. See TPRM Risk concentration map. |
| **Risk Ratings section** | |
| Computed risk rating | The calculated **Computed risk rating**.<br>The value is overall risk rating for the third party, calculated after the assessment by rolling up all of the TPR assessors' risk ratings. |
| Override risk rating | Option to override the computed rating.<br>If you select the check box, then specify the following values:<br>◦ Overridden risk rating. Select the new risk rating.<br>◦ Overridden on: The system auto-populates the date that the override occurred.<br>◦ Justification: Enter the reason that you overrode the value. |

## Third-party risk tiering assessments — Legacy process

Organizations use risk tiering to classify their third parties into categories of potential risk posed at the time of onboarding. The standard predefined risk tiers are None, Low, Minor, Moderate, High, and Critical. Each risk tier has associated assessment questions and document requests.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## The more complete IRQ process replaces tiering

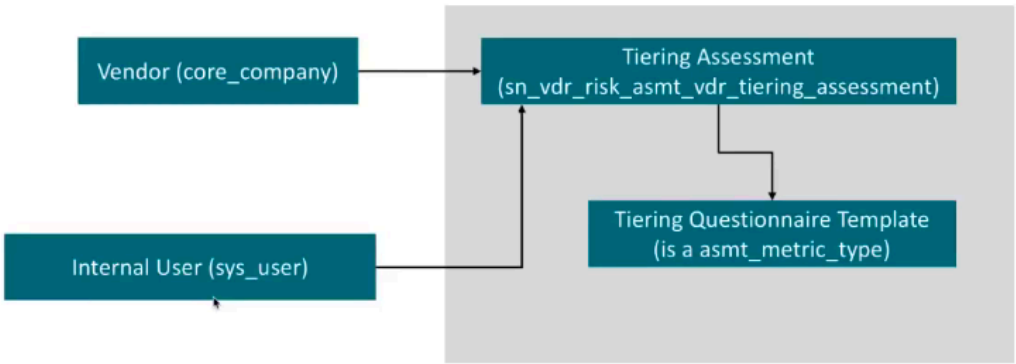
In the TPRM application, the IRQ is an internal questionnaire that improves the original tiering assessment process. IRQs enhance internal risk assessments with increased flexibility, control, and scalability.

To enable a seamless transition to TPRM, you have the option to duplicate existing tiering assessments and designate them as IRQ internal assessments. Risk tiering is supported as an unchanging legacy process.

## Legacy operation

1. Most organizations import their third-party portfolio through a spreadsheet or an integration with another onboarding solution. TPR managers make ongoing updates to third-party information, including risk security scores and risk tiers.
2. The TPR manager or TPR assessor determines the risk tier or categories of risk exposure for the third party.
3. The TPR manager selects the third party, assigns the tiering questionnaire template, and assigns the internal assessor that is required to complete the assessment. The third-party risk manager can assign a particular assessor to any specific section of the questionnaire.

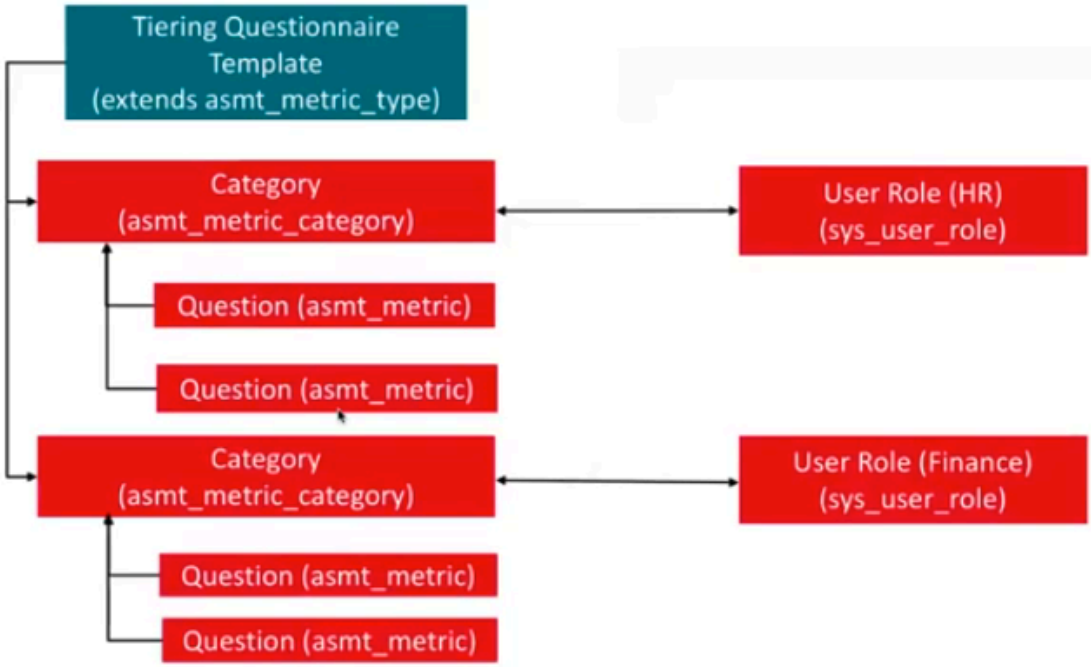
**Risk tiering assessment table relationship**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

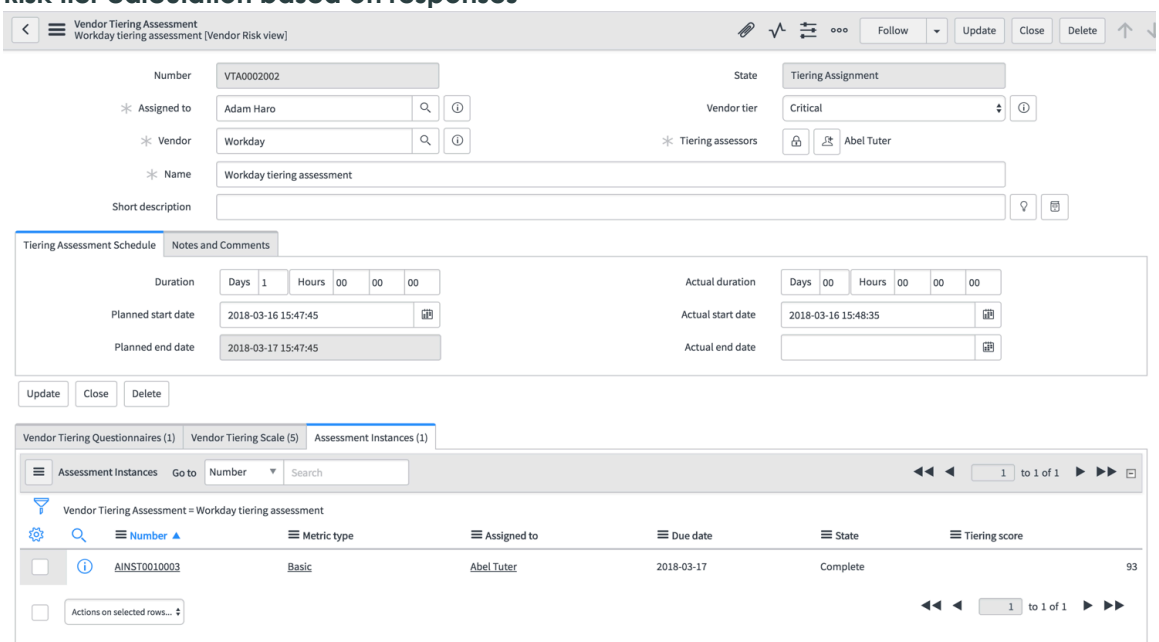
**Note:**

**Risk tiering questionnaire template table relationships for designated assessors**




4. Internal stakeholders navigate to **Self-service** > **My Assessments and Surveys** > to complete and submit the assessment.
5. After assessors have responded to the questionnaire, the system calculates the tiering score as the average of all scores. The TPR manager can initiate the risk assessment or a configured business rule can auto-send one. When the assessment is closed, the system assigns a risk tier to the third party based on the tiering score.

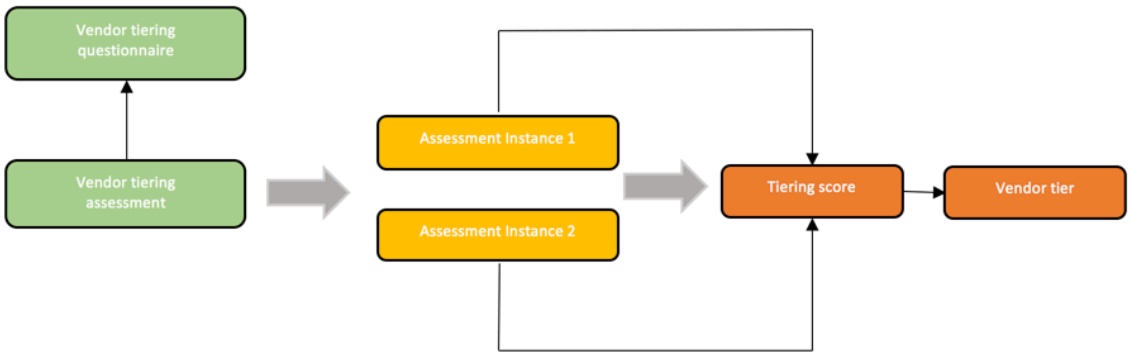
**Risk tier calculation based on responses**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Risk tiering scale and scoring calculations

### Risk tiering process




1. The tiering assessment initiates one assessment instance for each assigned assessor. The assessor sees only the sections assigned to them based on their role.
2. Response scores from all assessment instances are averaged to generate the tiering score.
3. The tiering score is mapped to risk tiers.
4. The risk tier is assigned to the third party when the tiering assessment is closed.

### Create and start a tiering assessment — Legacy process

The TPR assessor creates a tiering assessment from the vendor record, initiating the third-party risk tiering assessment life cycle. Also, third-party risk managers can select multiple third parties at a time and trigger multiple third-party risk tiering assessments.

#### Before you begin

Role required: sn_vdr_risk_asmt.vendor_assessor

#### About this task

The more complete IRQ process replaces tiering.

**Important:**

In the TPRM application, the IRQ is an internal questionnaire that improves the original tiering assessment process. IRQs enhance internal risk assessments with increased flexibility, control, and scalability.

To enable a seamless transition to TPRM, you have the option to duplicate existing tiering assessments and designate them as IRQ internal assessments. Risk tiering is supported as an unchanging legacy process.

#### Procedure

1. Use either of the following methods to start the process:
   - On the **Risk** tab of the Vendor Management Workspace, select **Create tiering assessment** in the Quick actions box.
   - Navigate to **All** > **Third-party Risk Management** > **Assessment Submission Rules** > **Tier Based Submission**.
2. Fill in the fields on the **Details** tab and then click **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Tiering Assessment section

| Field | Description |
|---|---|
| Name | Name of the tiering assessment. |
| Short description | Description of the tiering assessment. |
| Number | For each risk tiering assessment, the system auto-assigns a unique ID number that starts with the text **VTA**.<br><br>The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Applies to | The entity to which the assessment applies:<br>◦ **Third party**: The parent organization.<br>◦ **Engagement**: The organization within the third party that will supply the product or service. |
| Third party | Vendor being assessed. |
| State | ◦ Draft: Default value while the assessment is being defined.<br>◦ Awaiting Response<br>◦ Tiering Assignment<br>◦ Closed |
| Assigned to | TPR manager assigned to manage the tiering assessment process. |
| Tier level | Risk tier for the third party.<br>◦ Critical<br>◦ High<br>◦ Moderate<br>◦ Low<br>◦ Minor<br><br>The results of the tiering assessment and risk assessment help to determine the value. The TPR manager can override the value. |
| Tiering assessors | Internal assessors responsible for completing the tier assessment. |

### Tiering assessment schedule

| Field | Description |
|---|---|
| Tiering Assessment Schedule | |
| Planned duration | Estimated duration of the assessment. |
| Planned start date / Planned end date | Date and time that work on the tiering assessment is expected to begin and end. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Actual duration | Amount of time it took to complete the tiering assessment. This value is calculated using the **Actual state date** and **Actual end date**. |
| Actual start date / Actual end date | Date and time that work on the tiering assessment began and was completed |
| Notes and Comments | |
| Work notes | Information about the assessment process. Work notes are visible to users who are assigned to the issue. |
| Additional comments (Customer visible) | Public information about the third-party risk assessment. |

3. Click **Save**.

   The **Compose section** on the **Details** tab enables you to permanently add text to the record. The Activity section is updated with any actions on issues and tasks, submissions to TP contacts, and also with work notes and comments that users add to the record. Add text in the following fields as needed:

   - **Work notes (Private)**: Information about the third-party risk assessment. Work notes are visible only to internal users who are assigned to the process.
   - **Comments**: Comments about the third-party risk assessment are visible both to internal users and to third-party contacts.

4. Select the **Tiering Questionnaires** tab, select the questionnaires to use for the tiering assessment, and then click **Add** and click **Add**.

   **Note:** The base system includes a sample tiering questionnaire called **Basic**. Modify and save the questionnaire to meet your needs.

5. Click **Save**.
6. When all settings are correct, click **Submit Assessment**.

### Review tiering assessment responses — Legacy process

Starting with GRC: TPRM version 15.0.0, risk tiering is a legacy process that you do not need to perform. Instead, use the IRQ process in the Vendor Management Workspace.

#### Before you begin

Role required: sn_vdr_risk_asmt.vendor_assessor

#### About this task

The more complete IRQ process replaces tiering.

**Important:**

In the TPRM application, the IRQ is an internal questionnaire that improves the original tiering assessment process. IRQs enhance internal risk assessments with increased flexibility, control, and scalability.

To enable a seamless transition to TPRM, you have the option to duplicate existing tiering assessments and designate them as IRQ internal assessments. Risk tiering is supported as an unchanging legacy process.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The TPR assessor can view risk tiering assessment responses after the internal stakeholders have submitted their assessment and adjust the scoring appropriately.

### Procedure

1. Use either of the following methods to start the process:
   - In the Vendor Management Workspace, click the List icon (  ) and then navigate to **Tiering risk assessments** > **Open assigned to me**.
   - Navigate to **All** > **Third-party Risk Management** > **Tiering Assessments** > **My Open Assessments**.
2. Review, add, or change responses, as necessary.

#### Create an automated risk assessment when the assigned risk tier changes—Legacy process

Create a risk assessment when the risk changes for a third party by using a tier-based assessment submission rule. With this process, you can start reassessing the risk automatically if the source of the tier change is the engagement or third party.

### Before you begin
Role required: sn_vdr_risk_asmt.vendor_risk_manager

### About this task
The comprehensive Inherent Risk Questionnaire (IRQ) process replaces tiering.

**Important:**

In the TPRM application, the IRQ is an internal questionnaire that improves the original tiering assessment process. IRQs enhance internal risk assessments with increased flexibility, control, and scalability.

To enable a seamless transition to TPRM, you have the option to duplicate existing tiering assessments and designate them as IRQ internal assessments. Risk tiering is supported as an unchanging legacy process.

### Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Assessment Submission Rules** > **Tier Based Submission**.
2. Select a rule record or select **New**.
3. On the form, fill in the fields.

**Security Score Providers form**

| Field | Description |
|---|---|
| Third party | Name of the third party to apply the rule to. This rule also applies to the selected third party's engagements.<br><br>**Note:** Leave the field empty to apply the rule to all third parties and engagements. |
| Active | Option to turn a tier-based assessment submission rule on or off.<br><br>When you select the check box, the tier-based assessment submission rule is on. When you clear the check box, the rule is turned off. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** When all rules are turned off, the third-party risk assessments aren't automatically generated by tier changes. |
| Tier | Risk tier that should automatically generate an external risk assessment:<br>◦ None<br>◦ Critical<br>◦ High<br>◦ Moderate<br>◦ Low<br>◦ Minor |
| Assessment Template | Template to send when the risk tier scale changes to the tier that is specified in the rule. |
| Auto submit to third party | Option to automatically submit an external risk assessment to a third party or engagement after the external risk assessment is generated. If the option isn't selected, the external assessment stays in the **Draft** state after it's created. |

4. Select **Update**.

   When a change to the tier activates the rule, the system generates an external risk assessment and sends it out to either the third party or engagement. An external assessment is only sent to the source of the tier change. If the third party or engagement caused the tier to change, an external assessment is sent to both the third party and the engagement.

## Managing external risk assessments — Legacy process

Before the TPR manager closes an assessment, stakeholders create issues and tasks, usually during the **Generating observations** state. The TPR assessor assigns third parties as needed and communicates using comment streams to achieve closure on non-compliance. The third-party primary contact uses the Third-party portal to view all assessments.

## External risk assessment workflow

1. The TPR admin creates questionnaire and document request templates.
2. The TPR manager creates internal risk assessment and external risk assessment templates, and also creates the notifications associated with the workflow.
3. The TPR manager prepares and sends the IRQ to internal stakeholders.
4. Internal stakeholders complete and submit the assessment.
5. After receiving the completed risk tiering assessments, the TPR assessor updates and closes the tiering assessment.
6. The TPR manager sends the assessments to the third party's primary contact. External risk assessments can be sent automatically based on changes to a risk score or risk tier.
7. The third-party contact signs into the Third-party portal to complete the risk assessment.

   The Third-party portal displays a list of assessments and the status of each. From the portal, the primary contact can invite other third-party collaborators to complete portions of

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

the assessments. After other collaborators are identified, the primary contact submits the assessment.

8. The TPR assessor reviews the results of the assessments and closes each third-party assessment, creating issues for remediation as necessary. When an issue is created for a particular question, a visual indicator appears in the Third-party portal for the question.

   Remediating

   Remediating an issue means that the underlying issue causing the control failure or risk exposure will be fixed.

   Accepting

   Accepting an issue means you create an exception for a known control failure or risk. Controls that are **Accepted** remain in a non-compliant state until the control is reassessed. In this way, the issue can be used to document observations during audits.

Related topics

Life cycle states of a third-party (external) risk assessment

## Create an external risk assessment — Legacy process

Create an assessment and initiate the third-party risk assessment life cycle. An external risk assessment specifies the details for the third party or engagement and defines the plan for completing the assessment.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager or sn_vdr_risk_asmt.vendor_assessor

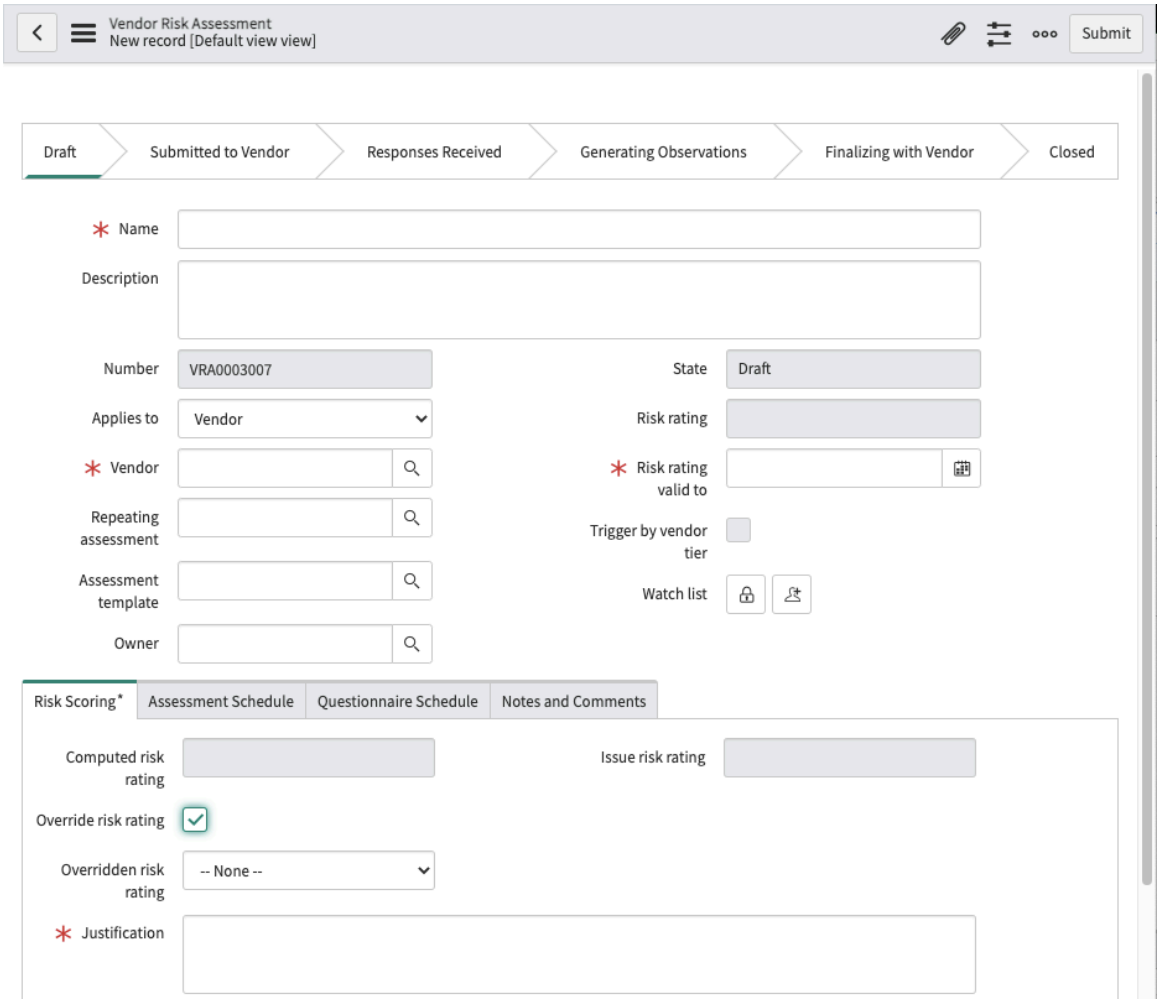
### About this task

Assessments can be created on-demand or can recur on a specified schedule. When creating an on-demand external risk assessment, TPR managers select the questionnaire template or document request template and the third party. TPR managers can select multiple third parties at a time and automatically trigger assessments.

### Procedure

1. Navigate to **All** > **Third-party Risk Management** > **External Risk Assessments** > **All Assessments**.
2. Select **New** and then fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




### Vendor Risk Assessment form

| Field | Description |
|---|---|
| Name | The name that identifies the third-party risk assessment on all forms and lists. |
| Description | A more detailed explanation of the issue. |
| Number | For each external risk assessment, the system auto-assigns a unique ID number that starts with the text **VRA**.<br><br>The unique ID is used in all references to the item. You can use the ID to search or filter for the item that you want to work on. |
| Applies to | The entity to which the assessment applies: **Third party** or **Engagement**. |
| Vendor | The assessed third party.<br><br>**Note:** You can reactivate a third party that is in **Terminated** status. If such a request is accepted and closed, the third party's status is changed to **Active**. |
| Engagement | Select the engagement to assess. The field is visible only if you selected **Engagement** from the **Applies to** field. |
| Repeating assessment | The assessment used to create the current assessment. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| Assessment template | Select an assessment template to create questionnaires or document requests for this assessment.<br><br>To use multiple templates to create multiple questionnaires or document requests for the assessment, leave the field empty. |
| Owner | The owner is the person who owns an assessment for audit purposes and monitors and manages overall assessment processes. Owners are responsible for confirming that the assessment is completed in a timely fashion by the third party, reviewing their responses, and creating and resolving issues. To drive the assessment to its completion, owners are notified when an assessment reaches a particular milestone. The owner must have the TPR manager or TPR assessor role.<br><br>For new requests, if the **Owner** field is empty, then the following action happens: The system sends an email notification to all users in the group that is specified in the **Assignment group**. The message states that the request was received and is in the **New** state. The message also includes a link to the details page for the request. See Add users to groups based on responsibilities.<br><br>**Note:** If the **Owner** field is empty and you select **Start the IRQ process**, then you become the owner. |
| Assignment group | For new requests, the **Assignment group** is set to **Due diligence request assigners**. The system sends an email notification to all users in the group that is specified in the **Assignment group**. The message states that the request was received and is in the **New** state. The message also includes a link to the details page for the request.<br><br>On the due diligence request form:<br><br>◦ Any member of the group can select **Assign to me** or set the **Owner** field to any other member of the group.<br>◦ A TPR manager or TPR assessor can clear the **Assignment group** field or change the value to select from different TPR assessors in the **Owner** selection list. |
| State | The process of collecting assessment data from a third party transitions through several states. See Life cycle states of a third-party (external) risk assessment for detailed descriptions. |
| Risk rating | The overall risk rating for the third party.<br>◦ Critical<br>◦ High<br>◦ Moderate<br>◦ Low<br>◦ Minor |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | **Note:** The **Risk rating** is determined by finding a risk rating scale range in which the risk score falls. It defines how a minimum and maximum range of assessment scores maps to a qualitative risk score. |
| Risk rating valid until | The date the risk rating expires. The date must be later than the **Risk rating valid to** date on any associated questionnaires or document requests. |
| Trigger by risk tier | Select the check box to initiate the assessment when the risk tier changes for the third party. |
| Watch list | Add users that should be notified when this record is modified. |
| **Risk Scoring**<br>**Note:** Risk ratings are calculated and displayed after assessment responses have been received. | |
| Computed risk rating | Average of the third-party risk area risk ratings. |
| Override risk rating | Select the check box to override the computed risk rating for the third party. When selected, future changes to the assessment risk rating will affect only the computed risk rating, not the risk rating.<br>**Note:** If you deselect a selected check box, then the computed risk rating is copied to the assessment. |
| Overridden risk rating | If you selected **Override risk rating**, enter the new risk rating. |
| Justification | If you selected **Override risk rating**, you must enter a reason for the override. |
| Issue risk rating | The risk rating for issues associated with the third parties being assessed. The issue risk rating is based on the priority of closed issues and how they were resolved.<br>◦ If the issue was **Closed Completed**, it indicates that the issue was resolved.<br>◦ If the issue was **Closed Incomplete**, it indicates that the third party failed to complete the associated questions.<br>◦ If the issue was **Closed Cancelled**, it indicates that the issue didn't need to be resolved.<br>If the issue is closed and the **State** of the assessment isn't closed or cancelled, the **Issue risk rating** is recalculated and displayed.<br>**Note:** The **Computed risk rating** isn't affected by this calculation. |
| Override risk rating | Option to override the computed risk rating for the third party. When selected, any future changes made to the assessment risk rating will affect only the computed risk rating, not the risk rating.<br>**Note:** If the check box is selected and then deselected, the computed risk rating is used. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

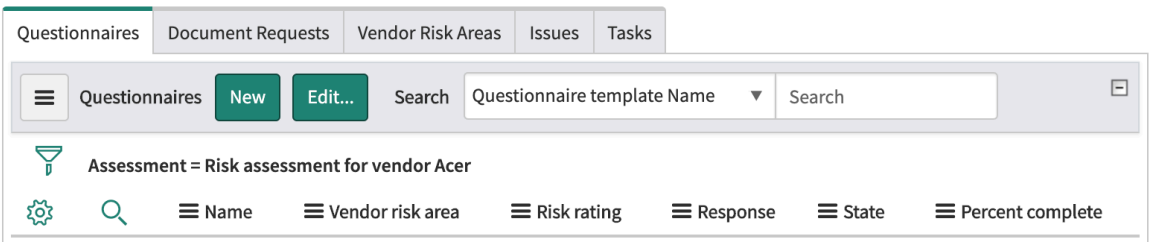
| Field | Description |
|---|---|
| Overridden risk rating | If you selected **Override risk rating**, enter the new risk rating. |
| Justification | If you selected **Override risk rating**, you must enter a reason for the override. |
| **Assessment Schedule** | |
| Planned duration (days) | Estimated duration of the assessment |
| Planned start date / Planned end date | Planned start and completion dates and times for work on the assessment. |
| Created by | User who created this record. |
| Created | Date/time the record was created. |
| Actual duration | The amount of time it took to complete the third-party risk assessment. This field is calculated using the **Actual state date** and **Actual end date**. |
| Actual start date | Date and time that work on the assessment began. |
| Actual end date | Completion date and time for the assessment. |
| Updated | Date/time when the record was last updated. |
| **Questionnaire Schedule** | |
| Planned duration (days) | The amount of time given to the third party to complete the assessment. The value is calculated using the **Planned state date** and **Planned end date**. |
| Review duration (days) | Time allocated for the customer to review all questionnaires. |
| Due date | Deadline for third party to respond to and return all questionnaires. |
| Completion date | Actual date when third party completed all questionnaires. |
| Submitted to vendor | Delivery date for third party questionnaires. |
| Resubmitted to vendor | Date that questionnaires are resent to the third party. |
| Responses expected by | The date that your organization expects the responses to be returned by the third-party contact. |
| **Notes and Comments** | |
| Work notes | Information about the assessment. Work notes are visible to users assigned to the issue. |
| Additional comments | Public information about the assessment. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| (Customer visible) | |

3. Save the record.

   Additional related lists appear. If you left the **Assessment template** field empty and want to use assessment templates to associate multiple questionnaires and/or document requests with this assessment, use the **Questionnaires** or **Document Requests** related lists.

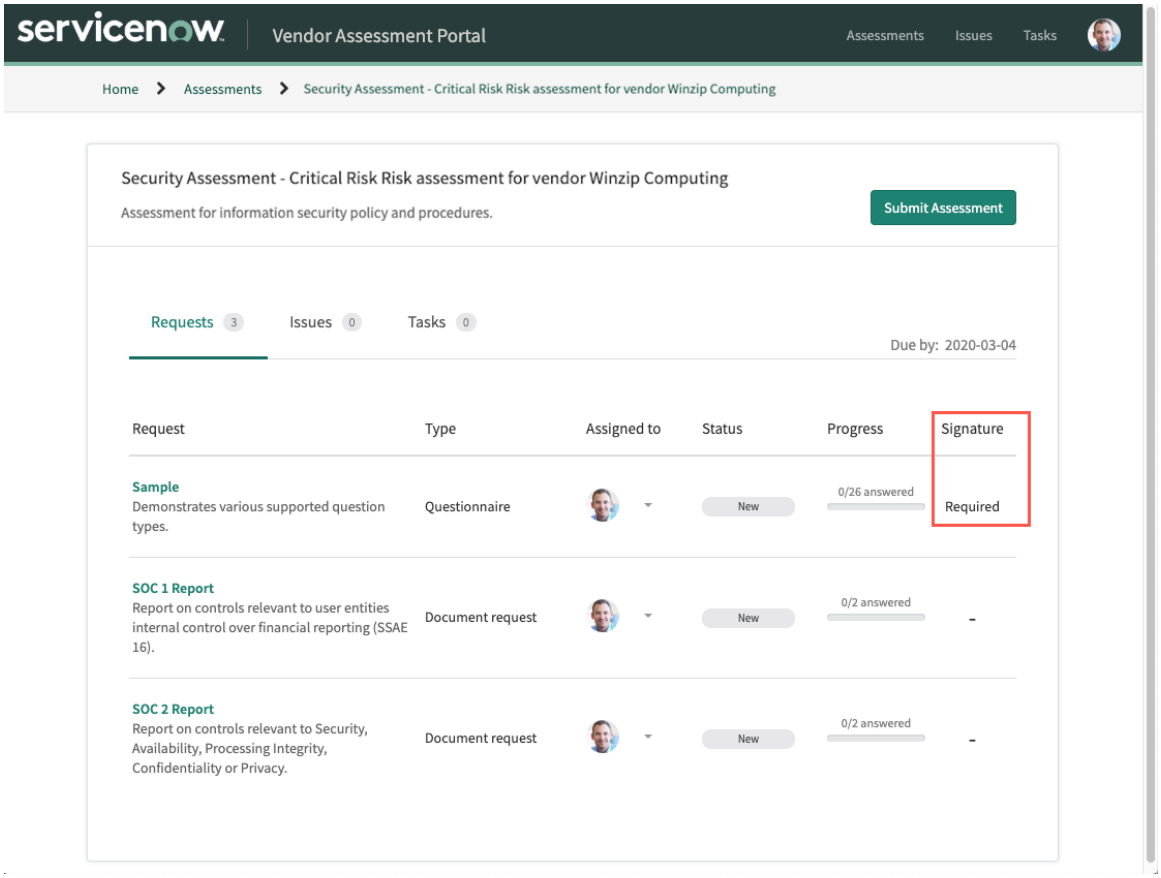



4. To associate existing questionnaires and/or document requests with the assessment, perform the following steps.
   a. Open the **Questionnaires** or **Document Requests** related list.
   b. Select **Edit**, select the questionnaires or document requests to use, and then select **Save**.
   c. Repeat for the other type of questions, if needed.
5. To create new questionnaire and/or document request templates and associate them with the assessment, see Create a questionnaire template or document request template.

> **Important:** In the next step, you can choose to submit the questionnaire to the third party. To pre-populate the questionnaire with responses from the most recently closed assessment, you must select the **Include previous responses** option before you submit it to the third party. The setting cannot be changed after the questionnaire is sent to the third party. See Create a questionnaire template or document request template.

6. Select **Submit to third party**.
   - The state of the assessment changes to **Submitted to third party**.
   - The templates that you selected generate questionnaires and/or document requests.
   - If the **Include previous responses** option is selected for a questionnaire, then previous responses are copied and added to the outgoing questionnaire. The notification in the Third-party portal includes the number, name, and closing date of the assessment that supplied the responses. The notification also includes a link to the assessment.
   - The primary third-party contact receives an email notification that includes a link to the assessment in the Third-party portal.
7. When the third-party contact is ready to respond to the assessment, they open the assessment in the Third-party portal.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**Note:** In the example, one of the questionnaires requires a signature. The third party or reviewer must save and e-sign the questionnaire or document request before it can be submitted. For more information, see E-signatures on questionnaires or document requests.

8. The TPR assessor moves the state of the assessment to **Generating Observations**.

   During this time, the TPR assessor can select the **View Response** link in the document **Document Requests** or **Questionnaires** related list to view the response and provide comments or change responses, as necessary.

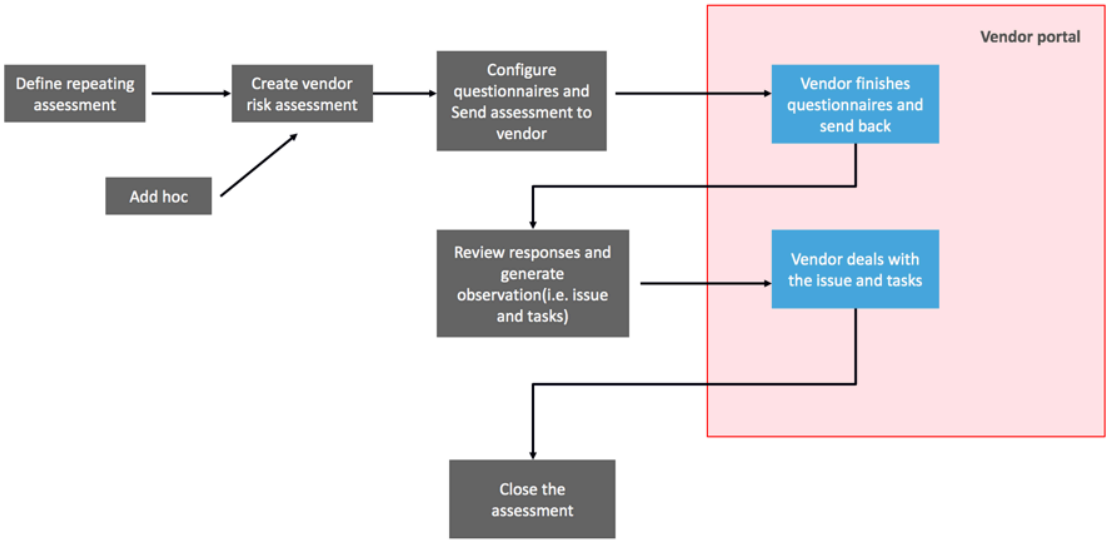
   For any problems that arise, the TPR assessor creates an issue to track the remediation process (Finalizing with third party).

9. The TPR assessor moves the assessment to **Closed** state.

### What to do next

The TPR assessor works through the third party portal with the third party to close the assessment.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




# Managing the Third-party portal

Third-party contacts respond to questionnaires, requests for documentation, tasks, and issues on the Third-party portal. The portal is the point of interaction between third parties and risk assessors.

## Third-party contacts

Third-party contacts are the individuals that represent the third party. By using the third-party portal, they can respond to questionnaires, work on tasks, and address issues that your third-party risk assessment team raises. Third-party contacts are either primary or secondary contacts. The primary contact is the assigned individual who receives the assessment questionnaires. Each third party must have at least one primary contact. The Third-party Risk (TPR) manager [sn_vdr_risk_asmt.vendor_risk_manager], TPR assessor [sn_vdr_risk_asmt.vendor_assessor], or the primary contact can create third-party contacts.

You assign the **primary contact** responsibility to the third-party contact who can directly answer assessment questions or assign another contact at the third party to answer the questions. Primary contacts can manage other contacts for the third party.

Third-party contacts are automatically assigned two roles: vendor_contact and snc_external. The vendor_contact role provides third-party contacts with access to the Third-party portal, while the snc_external role is a safeguard that restricts access only to the portal. The snc_external role helps prevent any unauthorized entry into your instance. For more information, see Set up third-party contacts.

**Note:** Third-party contacts see your organization's name in all references on the Third-party portal. You specify the name in the `sn_vdr_risk_asmt.company.name` property setting. See Configure TPRM properties.

## Tasks for third-party contacts

The primary third-party contact can perform the following tasks:

- Delegate questionnaires, tasks, and issues to other third-party contacts.
- View and update the third-party contact information.
- Update the notification preferences.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

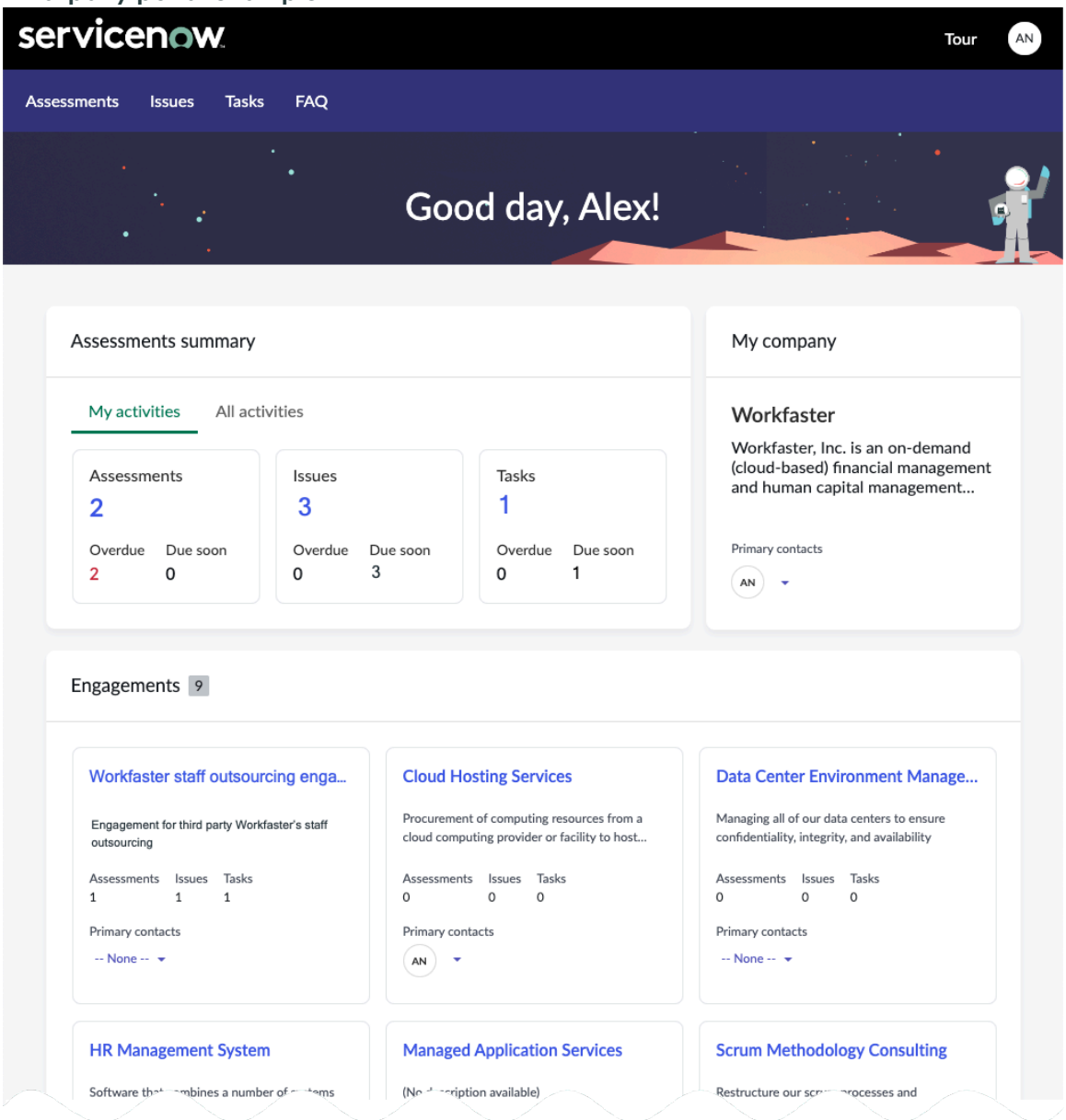
Secondary third-party contacts can use the portal to perform the following tasks:

- View and respond to "assigned to me" assessments.
- Change a password or request a new password.

**Important:** The third-party contact role should be used only for external contacts. The role prohibits access to the Now Platform and grants access only to the Third-party portal.

Third-party contacts see the portal as shown in the following example.

**Third-party portal example**




## Launching the portal

Third-party contacts launch the portal by using **[your instance URL]/svdp**).

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Learning to use the portal—the FAQ page

Third-party contacts can select **FAQ** to view answers to common questions, such as how to invite additional users to the portal and how to assign primary contacts to third-party or engagement records.

## Managing third-party contacts

Users in your organization with the Third-party risk assessor role [sn_vdr_risk_asmt.vendor_assessor] use TPRM to manage the following third-party contact activities:

- Create a login for a new third-party contact.
- Enable or disable a third-party contact login.
- Reset a password for a third-party contact.
- Assign a user role to a third-party contact.
- Assign a third-party contact to an assessment.
- View and update the customer contact information.
- Access the completed assessments.

For more information, see Set up third-party contacts.

Related topics

E-signatures on questionnaires or document requests

Using the SIG questionnaire for risk assessment

Using Supplier Collaboration Portal

## Set up third-party contacts

Set up your third-party contacts so that you can send assessments, address issues, and communicate any additional required information with these contacts.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_risk_manager and admin for steps 4 and 5

### About this task

Third-party contacts are external users at the third-party organization. They use the Third-party portal to securely organize, prioritize, and perform tasks like responding to questionnaires for assessments, performing tasks, and communicating with your risk-assessment staff regarding issues. You grant access to the Third-party portal and specify the permissions for third-party contacts. The third-party risk (TPR) manager must contact a team member with the admin role to complete steps 4 and 5.

**Important:** The third-party contact role should be used only for external contacts. The role prohibits access to your Now Platform instance and grants access only to the Third-party portal.

### Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Third Parties** > **Third-party Contacts** to determine whether a third-party contact has already been assigned.

   The number of contacts is listed for each third party.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. On the third party contacts page, select a third party to view the list of associated contacts.
   - To manage existing contacts:
     - Select each contact to verify that the contact is associated with the appropriate third party, is active, and, if applicable, is specified as the primary contact.

       **Note:** The questionnaires, document requests, and issues that are currently assigned to the contact are listed in the associated tab.

     - If you don't have the admin role, ask a user who does to verify that the vendor_contact role appears for the user on the Roles related list. If the user with the admin role can't see the Roles related list, they have to go to step 4. If the user with the admin role can't see the vendor_contact role listed for the user, they have to go to step 5.
   - To add a contact, select **New** and continue with the following steps.

   **Note:** It's normal for a contact to have the snc_external role because the vendor_contact role includes it.

3. On the form, fill in the fields.

**Third-party contact form**

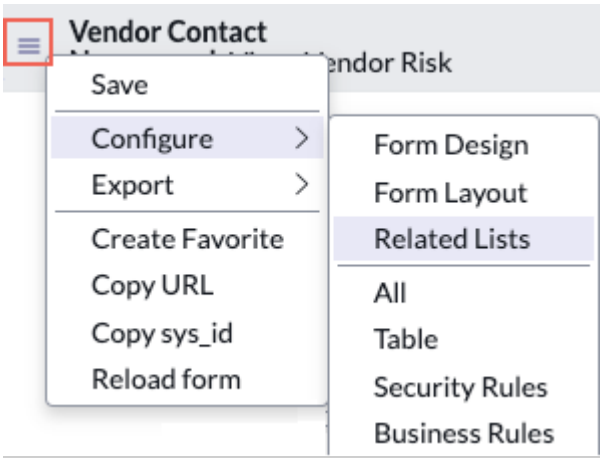
| Field | Description |
|---|---|
| First name, Last name, Email, Title, Department | Standard contact information for the user at the third-party organization. |
| User ID | ID used to log in to the Third-party portal instance. |
| Third-party | Third-party organization of the contact. |
| Language, Time Zone | Preferred language and time zone for the user at the third-party organization. |
| Active | Option to activate the contact to be eligible to work in the Third-party portal. |
| Primary contact | Third-party contact who can directly answer assessment questions or assign another contact at the third party to answer the questions. They can also manage other contacts for the third party. |

**Note:** An email notification is sent out to the new third-party contact after the form is submitted. The email contains a link to the third-party portal and login credentials.

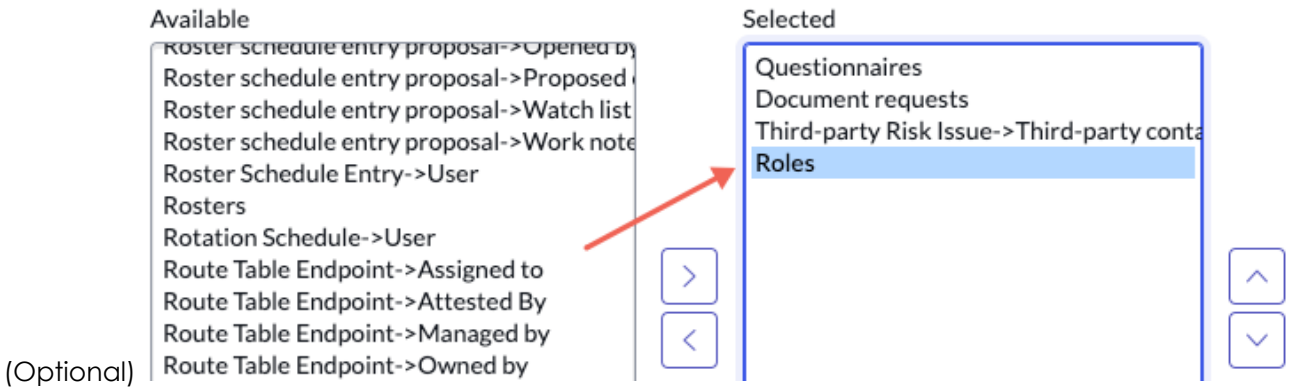
4. Optional: Validate that each contact has the vendor-contact role by adding the **Roles** value to the Vendor Contact page.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**a.** Add the Roles related list by selecting the actions icon and selecting **Configure** > **Related Lists**.



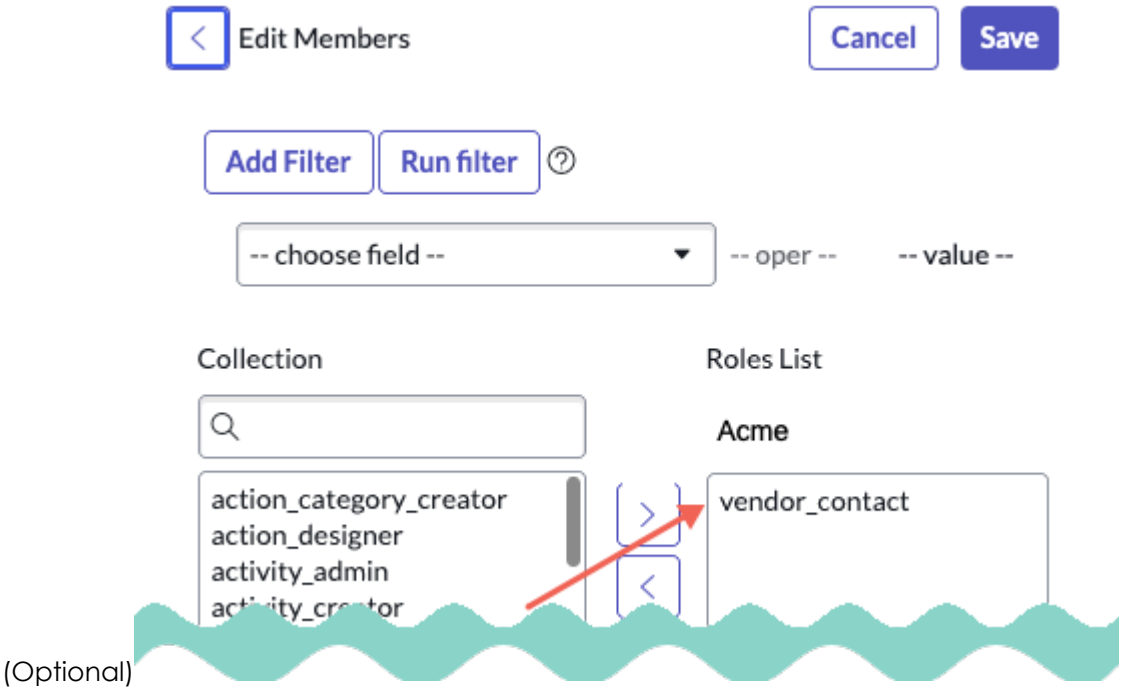

**b.** Move the Roles related list to the Selected list and then select **Save**.




(Optional)

**5.** Optional: Grant third-party contacts access to the third-party portal by selecting **Edit** and adding **vendor_contact** to the Roles list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




(Optional)

**Warning:** If the user has other roles, such as snc_internal, then the user might also be able to log in to your platform and have visibility into critical records.

## E-signatures on questionnaires or document requests

Questionnaires or document requests might require electronic signatures of third-party contacts and/or reviewers.

### Before you begin

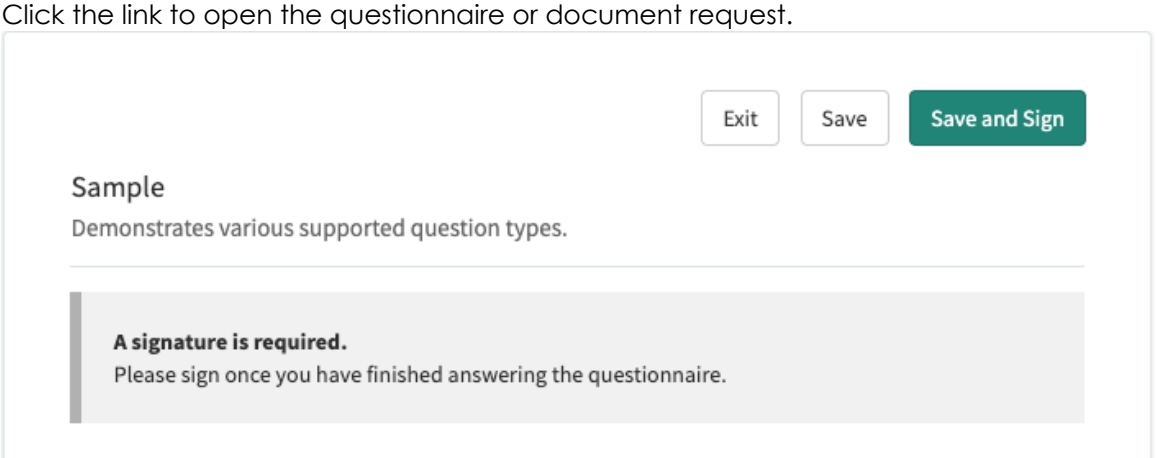
Role required: sn_vdr_risk_asmt.vendor_risk_manager or sn_vdr_risk_asmt.vendor_assessor

### About this task

After a questionnaire or document request has been submitted to the third party, the Third-party Risk (TPR) manager or TPR assessor receives an email notification that includes a link to the record.

### Procedure

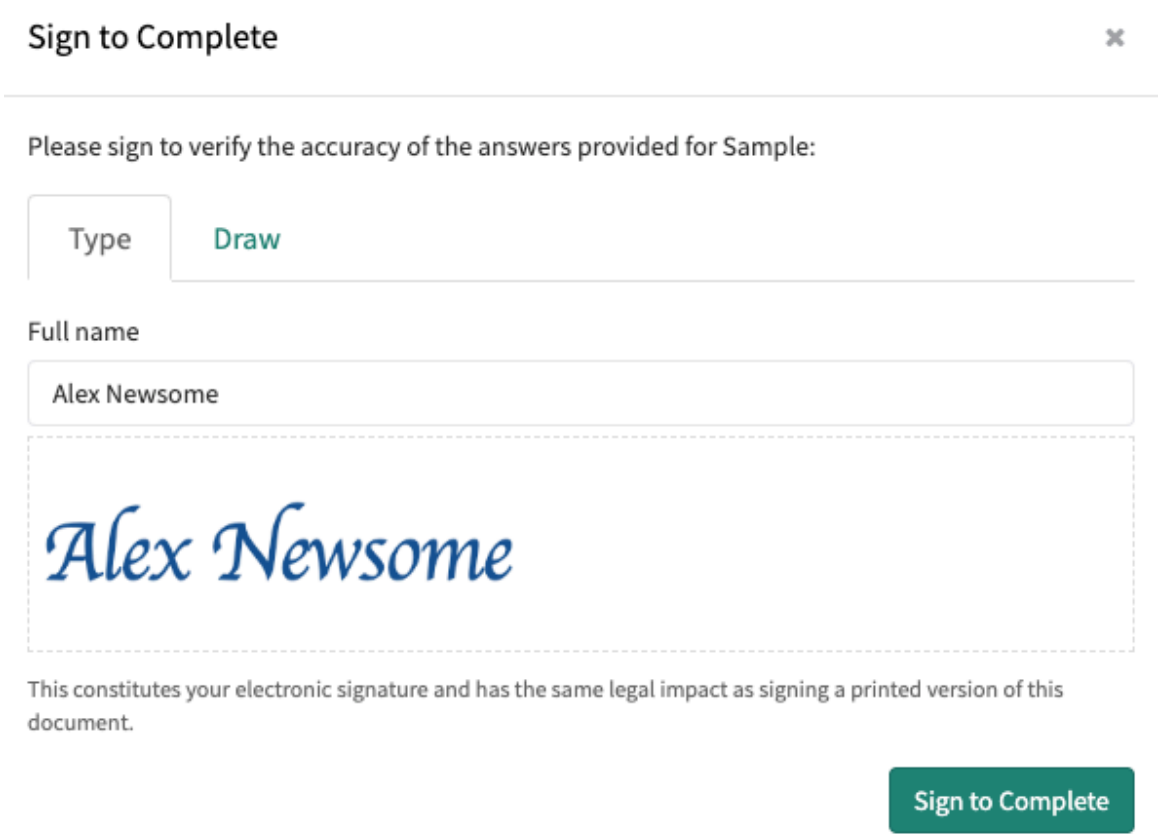
1. Click the link to open the questionnaire or document request.

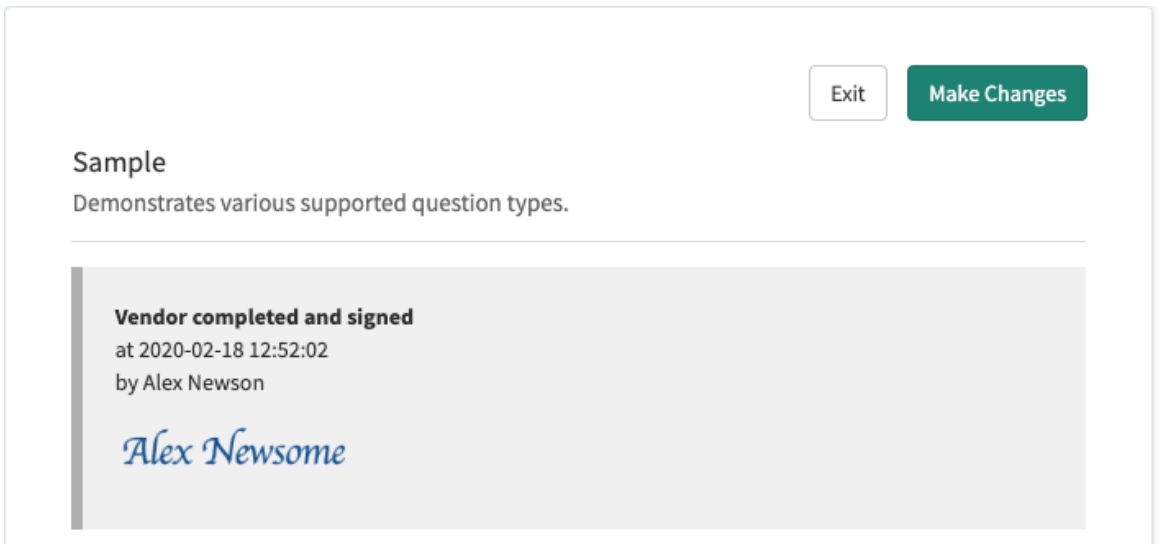



**Note:** Notice that a signature is required for the **Sample** questionnaire. Open the questionnaire that requires a signature.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. Complete the questionnaire or document request, and, when you have answered the questions, click **Save and Sign**.
3. Use the **Type** tab to enter your name or use the **Draw** tab provide a free-form signature and then click **Sign to Complete**.




4. To update the questionnaire or document request in any way, click **Make Changes**. The signature is removed and you must sign again after making the changes.
5. After you have completed and signed the assessment, click **Exit** and then repeat the process for any additional questionnaires or document requests in the assessment.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

6. When you have completed all questionnaires or document requests in the assessment, click **Submit Assessment**.

   **Note:** You cannot submit an assessment until all items that require e-signatures have been signed.

**Result**
The state of the assessment changes to **Response Received**, and risk scores are calculated.

## Using the SIG questionnaire for risk assessment

Third parties can use the Shared Assessments Standardized Information Gathering questionnaire (SIG) to provide assessment documentation. The third-party contact can upload the pre-filled SIG spreadsheet or respond to a form-based questionnaire that is imported to the instance.

## Supported SIG versions

TPRM supports the current SIG version and two prior versions. Supported SIG versions:

- SIG Full 2023, 2022, 2021
- SIG Core 2023, 2022, 2021
- SIG Lite 2023, 2022, 2021

**Important:**

The base system includes sample SIG questionnaires. ServiceNow doesn't provide the correct answers. The templates provided by Shared Assessments also don't include the correct answers. You determine what constitutes right and wrong answers.

Yes-or-no questions in the sample SIG questionnaires don't include scoring logic. By default, all **Yes** answers in the samples are graded as correct. You must configure the logic to suit your needs.

## How third parties can use the SIG

- If a third party uploads a version prior to the earliest supported SIG, all responses for matching questions are imported and any non-matching questions are imported with empty responses for the third party to answer later.
- If a third party attempts to load data from a version of SIG that is older than the current version, some questions might not be mapped or parsed correctly (for example, if you load data for SIG 2020 full on SIG 2021 full).
- Loading a version of SIG prior to 2021 isn't supported.

For instructions that you can send to third-party contacts, see Third-party contacts — Respond using the SIG.

Related topics

Third-party contacts — Respond using the SIG

### Third-party contacts — Respond using the SIG

As the contact who is responding to a risk assessment, you can use the Shared Assessments Standardized Information Gathering questionnaire (SIG) to provide assessment documentation. Upload the pre-filled SIG spreadsheet or import a form-based questionnaire.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: vendor_contact

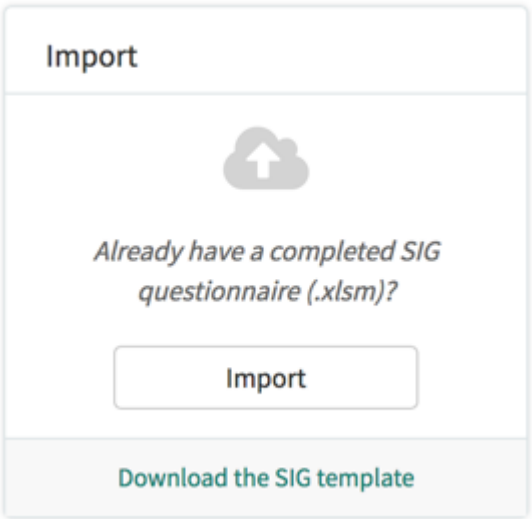
### About this task
TPRM supports the current SIG version and two prior versions. Supported SIG versions:

- SIG Full 2023, 2022, 2021
- SIG Core 2023, 2022, 2021
- SIG Lite 2023, 2022, 2021

If you upload a version prior to the earliest supported SIG, all responses for matching questions are imported and any non-matching questions are imported with blank responses for you to answer later.

**Important:** If you attempt to load data from a version of SIG that is older than the current version, some questions might not be mapped or parsed correctly (for example, if you load data for SIG 2022 full on SIG 2023 full). You cannot load a version of SIG prior to 2021.

### Procedure
1. Log into the Third-party portal at `https://<myCompany>.service-now.com/svdp`.
2. Perform one of the following actions.

| Action | Steps |
|---|---|
| To upload a completed SIG questionnaire | Click **Import**, navigate to the file, and then click **Open**.<br>  |
| To download a blank SIG questionnaire | Click **Download the SIG template**.<br>**Note:** After completing the SIG questionnaire, click **Import**, navigate to the file, and then click **Open**. |

3. Complete the SIG questionnaire.
4. Submit the SIG questionnaire on the Third-party portal.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Integrating scores from risk intelligence providers

Risk intelligence providers generate risk scores for a variety of third-party risk domains. Your organization can purchase services from providers that return data that is analogous to personal credit scores. The scores provide insight on how trustworthy and safe a particular third party can be.

## Working with data from risk intelligence providers

**Note:** You can request risk data for third parties but not for engagements.

- After you register a risk intelligence provider, you specify which of the provider's scoring or rating services you'll use. You also specify how their scores or ratings map to your TPRM ratings.
- You add a raw score from a provider to the provider service record for a third party. The system uses the mapping that you specified to normalize the value to the appropriate TPRM rating.
- A provider-based submission rule is a set of conditions and actions. In a rule, you can specify that an update to a rating from a risk intelligence provider is the condition that triggers the action that is specified in the rule. The action might be to create and send a third-party risk assessment, issue, task, or email.

## Integrations supported by ServiceNow

**Note:** You will find the integration apps on the ServiceNow Store.

**Integrations supported by ServiceNow**

| Provider | Product name | Content | Service provided | Type |
|---|---|---|---|---|
| Standard Assessment | Standard information-gathering (SIG) questionnaire | Standard assessment | Industry standard questionnaire for use in assessments. | Content |
| Ecovadis | Ecovadis | Sustainability ratings | Sustainability scores in support of assessments and continuous monitoring. | ISV, data, ESG |

## Integrations supported by ServiceNow partners

**Note:** You will find the integration apps on the ServiceNow Store.

**Integrations supported by partners**

| Provider | Product name | Content | Use case | Type |
|---|---|---|---|---|
| BitSight | BitSight | Cyber risk ratings | Cyber risk scores in support of assessments and continuous | ISV, data |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Integrations supported by partners (continued)**

| Provider | Product name | Content | Use case | Type |
|---|---|---|---|---|
| | | | third-party risk monitoring. | |
| Security Scorecard | Security Scorecard | Cyber risk ratings | Cyber risk scores in support of assessments and continuous third-party risk monitoring. | ISV, data |
| riskrecon | Risk Recon | Cyber risk ratings | Cyber risk scores in support of assessments and continuous third-party risk monitoring. | ISV, data |
| Upguard | Upguard Vendor Risk | Cyber risk | Cyber risk scores in support of assessments and continuous third-party risk monitoring. | ISV, data |
| Recorded Future | Recorded Future Intelligence | Cyber risk ratings | Cyber risk scores in support of assessments and continuous third-party risk monitoring. | ISV, data |
| Black Kite | Black Kite | Third-party risk management | Technical security, financial risk, ransomware susceptibility index, and compliance scores in addition to overall security ratings. | ISV |
| Interos | Interos | Supply chain and multiple domain ratings | Cyber, financial, ESG, geopolitical, operations, and restrictions ratings to support risk assessments and monitoring. | ISV, content |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Integrations supported by partners (continued)**

| Provider | Product name | Content | Use case | Type |
|---|---|---|---|---|
| TruSight | TruSight | Third party risk assessments | Access to TruSight-validated third party risk assessments. | ISV |
| cyberGRX | CyberGRX | Third party risk assessments | Access to CuberGRX's third-party risk exchange to help automate assessments. | ISV |

Related topics

Viewing risk intelligence scores

Register a risk intelligence provider

## Register a risk intelligence provider

Create a record for each risk intelligence provider from which you'll request reports. The risk scores and ratings that risk intelligence providers generate are analogous to personal credit scores. The scores provide insight on how trustworthy and safe a particular third party can be.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_assessment_reviewer

### Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Risk Intelligence Provider Setup** > **Providers**.
2. Click **New**, fill in the form, and then click **Submit**.

**Risk intelligence providers form**

| Field | Description |
|---|---|
| Name | Unique name of the risk intelligence provider. |
| Short description | Description of the provider and possibly of the services provided. |
| Is multi-factor | Option to specify that the provider can return multiple different score types, for example, Financial risk or Security risk. |
| URL | Provider's website URL. This enables colleagues to visit and review the provider. |
| Note | Text comments that provide additional information for your colleagues, for example, descriptions of the available scoring services or why your organization has decided to use the provider. |
| Provider logo | Image of the provider's logo. This image appears on TPRM reports for the provider. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Result
You can now specify the services and levels of service that you might later request from the provider.

Services that you have associated with the provider appear in the **Risk intelligence provider services** related list. To add a service, click **New** in the related list and then follow the instructions in Set up a risk intelligence provider service.

## Set up a risk intelligence provider service

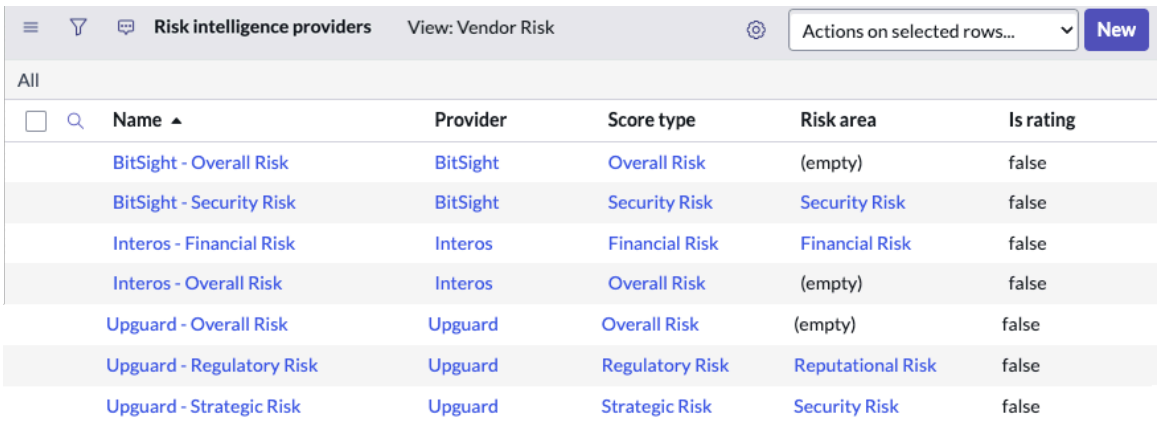
After you register a risk intelligence provider, you specify which of the provider's scoring or rating services you'll use. You also specify how their scores or ratings map to your TPRM ratings.

### Before you begin
Role required: vendor_assessment_reviewer

### Procedure
1. Navigate to **All** > **Third-party Risk Management** > **Risk Intelligence Provider Setup** > **Provider Services**.

   Current risk intelligence provider services appear in the **Third-party Provider Services** related list.

   **Note:** The list of provider services also appears as a related list while you are registering a provider. The system auto-generates a unique name for the service by concatenating the **Provider** name and **Score type**.




| Name | Provider | Score type | Risk area | Is rating |
|---|---|---|---|---|
| BitSight - Overall Risk | BitSight | Overall Risk | (empty) | false |
| BitSight - Security Risk | BitSight | Security Risk | Security Risk | false |
| Interos - Financial Risk | Interos | Financial Risk | Financial Risk | false |
| Interos - Overall Risk | Interos | Overall Risk | (empty) | false |
| Upguard - Overall Risk | Upguard | Overall Risk | (empty) | false |
| Upguard - Regulatory Risk | Upguard | Regulatory Risk | Reputational Risk | false |
| Upguard - Strategic Risk | Upguard | Strategic Risk | Security Risk | false |

2. Click **New** and then fill in the fields on the form.

#### Risk Intelligence Provider Service form

| Field | Description |
|---|---|
| Provider | Name of the risk intelligence provider for this scoring service. |
| Score type | Each service offered by the provider returns a particular type of risk rating or score, for example, Financial risk or Security risk.<br><br>For each provider, you define at least two services. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

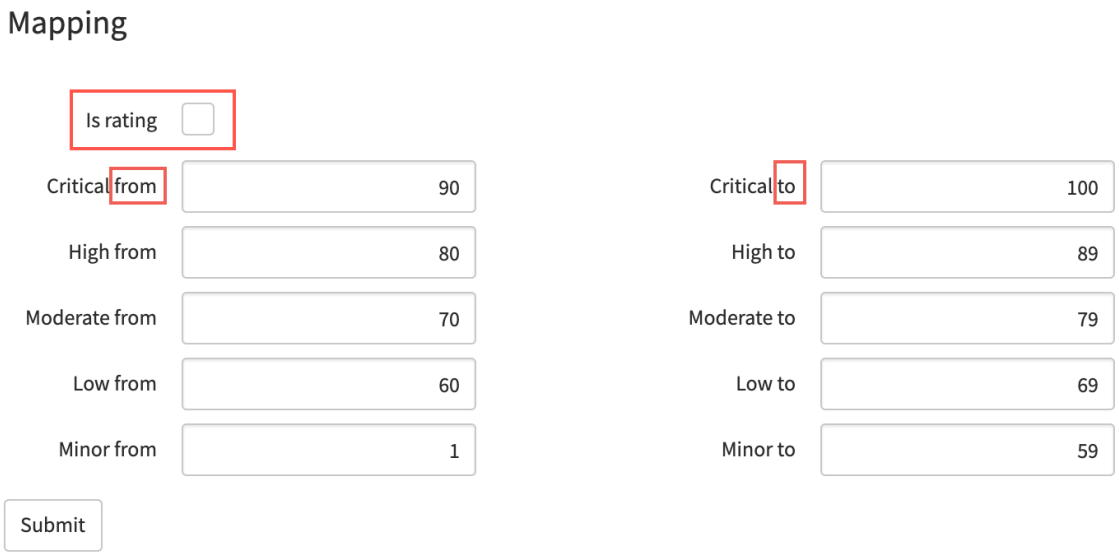
| Field | Description |
| --- | --- |
| | ◦ Define a service that returns the overall risk score for the third party.<br>◦ Define a service for each additional type of score that the provider can return.<br><br>**Important:**<br>◦ The **Is multi-factor** setting for a provider indicates that the provider can return multiple different score types. For providers that you configure as multi-factor, you must define a service with **Score type** = **Overall Score** before you can create other services for the provider. When the provider returns an overall score, you add the data. The normalized value appears as the "Overall" value on the provider's card on the**Risk intelligence scores** tab.<br>◦ For providers that you configure as not multi-factor, you specify only one score type. The score or rating returned by the provider is converted to the normalized TPRM score. The normalized value is also displayed as the "Overall" value on the provider's card on the**Risk intelligence scores** tab. |
| Name | Name of the provider service being set up.<br><br>The system auto-generates a unique name for the service by concatenating the **Provider** name and **Score type**. |
| Risk area | Select the third-party risk domain associated with the score type.<br><br>For more information, see Define a third-party risk domain.<br><br>**Note:** Risk domains are called "risk areas" in some platform applications. |
| Copy mapping from | If applicable, specify an existing service with this provider that uses identical mapping as the service that you are configuring.<br>◦ The mappings are copied to the current record.<br>◦ The mappings become read-only. |

3. Scroll to the **Mapping** area and perform one of the following actions.
   - To map the provider ratings to the ratings used by TPRM, select the **Is rating** check box and then enter each provider rating next to its corresponding platform rating.
   - To associate a range of provider scores with each TPRM rating, do not select **Is rating**. Each row identifies the lowest and highest values in a rating. Enter the lowest value in the **from** column and the highest value in the **to** column.

   You must fill in at least three rows.

   - All rows must be either ratings or ranges. A mix of the two types is not allowed.
   - If there are more returned values than rows, group values in the appropriate row and separate with commas.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




4. Click **Submit**.
   In the following steps, you specify the available request types. A request type is the level of analysis for the **Score type** that you specified for the service. For example, a provider might offer three request types for the Financial Risk score type: Level 1, Level 2, and Level 3. A "Level 3" report might return significantly more detailed information and might cost significantly more than a "Level 1" report.
5. Navigate to **All** > **Third-party Risk Management** > **Risk Intelligence Provider Setup** > **Request Types** and then click **New**.
6. Select the provider, enter a request type, click **Submit**, and then repeat the process for each request type.
7. Repeat the overall process to define a service for each additional type of score that the provider can return.

### Result
You can now request a risk score from the risk intelligence provider.

## Add a risk intelligence score to risk data for a third party

You add a raw score from a provider to the provider service record for a third party. The system uses the mapping that you specified to normalize the value to the appropriate TPRM rating.

### Before you begin
Role required: sn_vdr_risk_asmt.vendor_assessment_reviewer

### About this task
You typically populate the risk intelligence scores table using an integration that you created or installed from the ServiceNow Store. This procedure describes the process of updating risk intelligence scores manually.

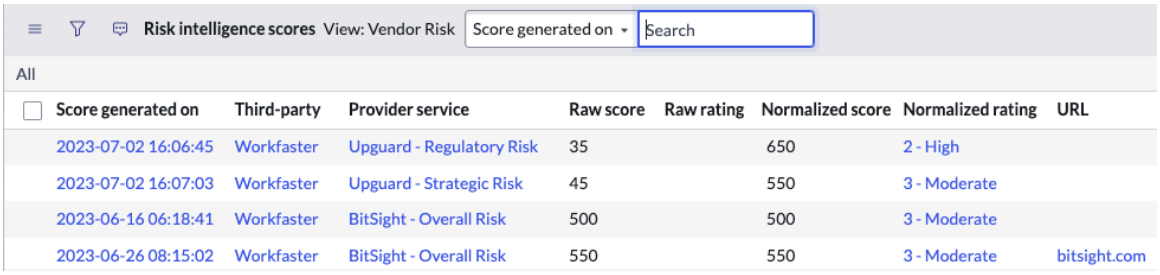
When you request a risk score for a third party, risk intelligence providers return the score at a URL that they specify. Follow this procedure to manually add the score and URL to your risk data for the third party.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **Third-party Risk Management** > **Risk Intelligence Provider Setup** > **Scores**.

   The Risk intelligence scores related list displays the list of current provider services and associated scores.




| Score generated on | Third-party | Provider service | Raw score | Raw rating | Normalized score | Normalized rating | URL |
|---|---|---|---|---|---|---|---|
| 2023-07-02 16:06:45 | Workfaster | Upguard - Regulatory Risk | 35 | | 650 | 2 - High | |
| 2023-07-02 16:07:03 | Workfaster | Upguard - Strategic Risk | 45 | | 550 | 3 - Moderate | |
| 2023-06-16 06:18:41 | Workfaster | BitSight - Overall Risk | 500 | | 500 | 3 - Moderate | |
| 2023-06-26 08:15:02 | Workfaster | BitSight - Overall Risk | 550 | | 550 | 3 - Moderate | bitsight.com |

2. Click **New**, fill in the fields on the Risk intelligence score form, and then click **Submit**.

   This step adds the score and the URL where the provider returned the score to the data for the third party or engagement.

   When you enter a rating from a risk intelligence provider, the system normalizes the value to convert it to the appropriate TPRM rating. When you enter a score from a risk intelligence provider, the TPRM generates both a normalized rating and a normalized numerical score.

### Risk intelligence score form

| Field | Description |
|---|---|
| Provider | Unique name of the risk intelligence provider. The choice list is populated with the providers that you registered. |
| Provider service | A name that is the concatenation of the risk intelligence provider name and the particular service that returned the risk data. You configured the service using the process specified in Set up a risk intelligence provider service. |
| Third party | Third party that was scored by the provider. |
| Request type | Level of analysis for the **Score type** that you defined for the service.<br><br>For example, a provider might offer three request types for the Financial Risk score type: Level 1, Level 2, and Level 3. A "Level 3" report might return significantly more detailed information and might cost significantly more than a "Level 1" report. |
| URL | URL of the site that the provider returned for the request.<br><br>The site provides the rating or score and additional information from the provider. |
| Raw rating / Raw score | Raw value returned by the provider in the specified URL. |
| Normalized score | If you entered a numerical raw score from the provider, then this is the computed normalized TPRM score. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Normalized rating | If you entered a numerical raw score or raw rating from the provider, then this is the computed normalized TPRM rating. |
| Score generated on | Date and time that the score was added to this record.<br>**Note:** This is not the date/time when the data was generated by the provider. |

3. Optional: Add subfactor data to the risk data for the third-party.
Subfactor data is not validated or mapped to TPRM score/rating data, but is stored directly as you enter it.

   a. Navigate to **All** > **Third-party Risk Management** > **Risk Intelligence Provider Setup** > **Subfactors** and then click **New**.

   b. Fill in the form in the same way as you filled in the data for a score/rating.

**Risk intelligence subfactors form**

| Field | Description |
|---|---|
| Provider | Unique name of the risk intelligence provider. The choice list is populated with the providers that you registered. |
| Provider service | A name that is the concatenation of the risk intelligence provider name and the particular service that returned the risk data. You configured the service using the process specified in Set up a risk intelligence provider service. |
| Name | Name of the subfactor. |
| Third party | Third party that was scored by the provider. |
| Score | Raw value returned by the provider.<br>**Note:** You can enter numerical or alphabetic text in this field. The value is not validated. |
| Created | (Optional) Date and time that the score was added to this record.<br>**Note:** This is not the date and time when the data was generated by the provider. |

**Result**

The data that you have associated with the third party now appears in reports. See Viewing risk intelligence scores for details. The data appears in the following locations:

- Risk intelligence scores related list as described in this procedure.
- **Risk overview** tab in the workspace.
- **Risk intelligence scores** tab in the workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Automate actions upon risk intelligence updates

A provider-based submission rule is a set of conditions and actions. In a rule, you can specify that an update to a rating from a risk intelligence provider is the condition that triggers the action that is specified in the rule. The action might be to create and send a third-party risk assessment, issue, task, or email.

### Before you begin

Role required: sn_vdr_risk_asmt.vendor_assessment_reviewer

### About this task

When you enter a rating from a risk intelligence provider, the system normalizes the value to convert it to the appropriate TPRM rating. When you enter a score from a risk intelligence provider, the TPRM generates both a normalized rating and a normalized numerical score.

Follow this procedure to define a rule to perform an action when a provider sends an updated rating or score.

### Procedure

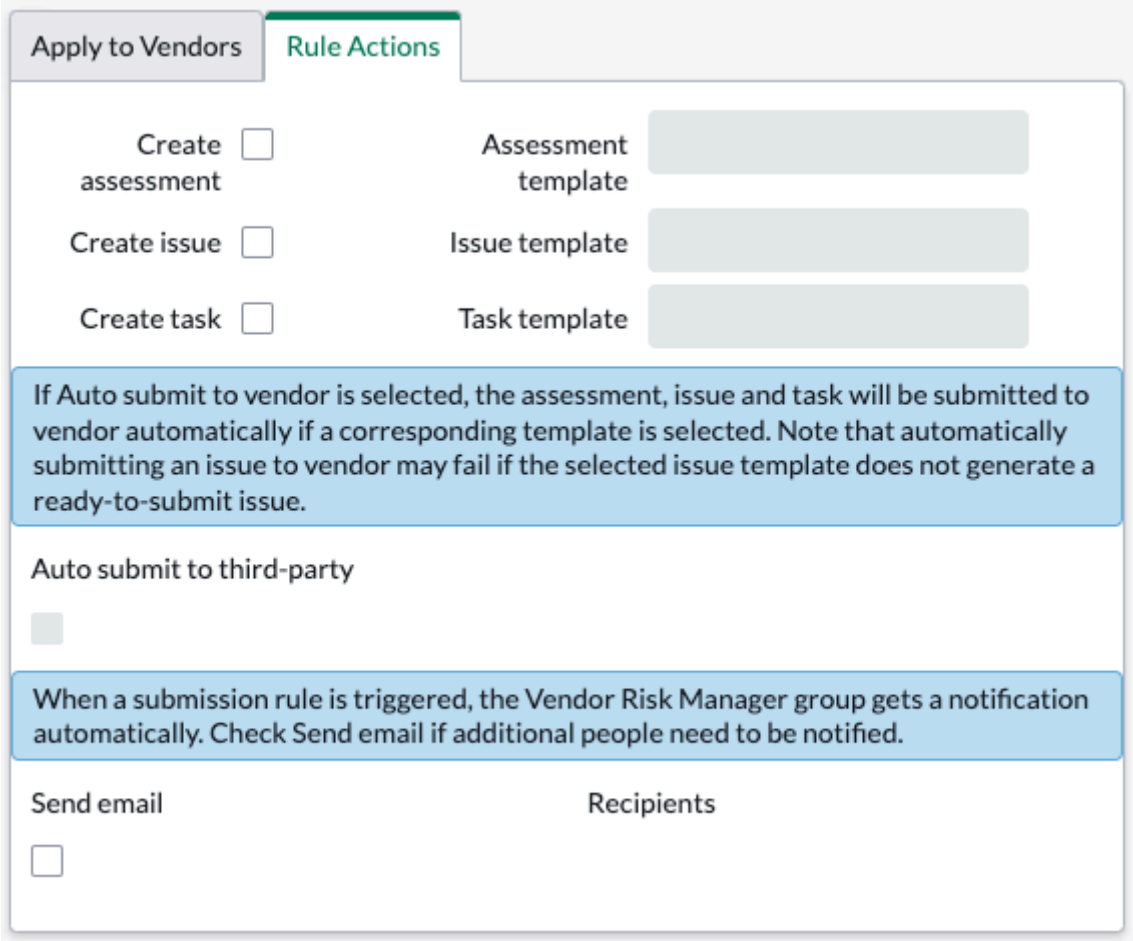
1. Navigate to **All** > **Third-party Risk Management** > **Assessment Submission Rules** > **Provider-based Submission**.
2. Click **New** and then fill in the form.

**Provider-based submission rule form**

| Field | Description |
|---|---|
| Provider service | Select the scoring service from the risk intelligence provider that is associated with the rule. |
| Order | Enter the execution order for the rule. If multiple rules are defined for the same risk intelligence provider, only the rule with the lowest **Order** value is executed. |
| Name | Auto-generated name of the rule. |
| ◦ Change type<br>◦ Extent of change<br>◦ Normalized percentage/ Normalized score/ Normalized risk rating | Select the basis for the external score change that should trigger the rule and the extent of change, as follows:<br>◦ If Change type = Normalized percentage, select **Increased risk by** or **Decreased risk by**, and the percentage in the **Normalized percentage** field.<br>◦ If Change type = Normalized score, select **Increased risk by**, **Decreased risk by**, or **Threshold**, and a score in the **Normalized score** field.<br>◦ If Change type = Normalized rating, enter a risk rating threshold that will trigger the rule in the **Normalized risk rating** field. |

3. Select the **Apply to Vendors** tab.
   a. Use the condition builder to define conditions for identifying the third parties to be affected by the rule.
   b. Click **Submit**.
4. Select the **Rule Actions** tab, fill in the fields, and then click **Submit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**Provider-based submission rule form — Rule Actions tab**

| Field | Description |
|---|---|
| Create assessment | Select this check box to create an assessment for the third parties identified on the **Apply to Vendors** tab. If you also select the **Auto submit to third party** check box, the assessment is automatically sent to the third parties when the rule is triggered. |
| Create issue | Select this check box to create an issue for the third parties identified on the **Apply to Vendors** tab. If you also select the **Auto submit to third party** check box, and you have selected a template from the **Issue template** field, the issues are auto-generated for the third parties when the rule is triggered.<br><br>**Note:** To enable to auto-generation, you must verify that the following three fields are completed when the issue is created:<br>◦ **Vendor**<br>◦ **Recommendation** (on the **Recommendations** tab)<br>◦ **Explanation** (on the **Recommendations** tab) |
| Create task | Select this check box to create a task for the third parties identified on the **Apply to Vendors** tab. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | If you also select the **Auto submit to third party** check box, and you have selected a template from the **Task template** field, the tasks are automatically created for the third parties when the rule is triggered. |
| Assessment template | If you selected the **Create assessment** check box, select the assessment template to be used to create the assessments. |
| Issue template | If you selected the **Create issue** check box, you can optionally select an issue template to be used to create an issue for the third parties identified on the **Apply to Vendors** tab.<br><br>If you also select the **Auto submit to third party** check box, you must select an issue template in order to automatically create an issue when the rule is triggered. |
| Task template | If you selected the **Create task** check box, you can optionally select a task template to be used to create a task for the third parties identified on the **Apply to Vendors** tab.<br><br>If you also select the **Auto submit to third party** check box, you must select a task template in order to automatically create a task when the rule is triggered. |
| Auto submit to third party | Automatically submit assessments, issues, and/or tasks to the third parties identified on the **Apply to Vendors** tab as described in the preceding field descriptions. |
| Send email/ Recipients | When the rule is triggered, users with the TPR manager role receive an email notification. Select **Send email** and specify **Recipients** to send the email notification to other individuals. |

## Third-party Risk Management reference

Reference topics provide detailed descriptions of tables, properties, forms, and roles that are installed with the Third-party Risk Management application.

### Terminology

Learn more about the key concepts and terms that are used in the TPRM application.

### Due diligence request process management

From the Details tab, you can view and adjust the due diligence request information. You can also log external-facing comments and private work notes, attach files, and track request updates in the activity stream.

### IRQ process management

The first internal step after an engagement request is approved is to start the IRQ process to scope the risk by determining the third party's risk score.

### Third-party (external) risk assessment management

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After the IRQ process is complete, you send questionnaires and document requests to the third-party contact. You manage the third-party risk assessment by working with the contacts to help ensure that the responses are complete and accurate.

### Request third-party risk due diligence request form

The due diligence request form captures all the initial information that you need to start the due diligence process. Any employee within your organization can request due diligence. If you're selecting an existing third party, a significant portion of the information is automatically filled in.

### Domain separation and Third-party Risk Management

Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

### Life cycle states of a third-party (external) risk assessment

The process of collecting assessment data from a third party moves between several states. For example, during the **Submitted to third party** state, the third party responds to tasks, issues, and works to complete the questionnaires.

### Third-party risk ratings and scoring calculations

Perform a comprehensive external risk assessment when calculating multiple ratings and scores by using the Third-party Risk Management application. You can gain a deeper understanding of the overall calculation process and learn how user-defined parameters and configurations influence the results of the questionnaires.

### Guidelines for importing spreadsheet data

Before you try to import the questionnaire data from a Microsoft Excel spreadsheet into Third-party Risk Management tables, you must verify that its format meets particular guidelines.

### Unique ID numbers for TPRM records

When you create (or the system generates) a new record (for example, a request for due diligence or a task), the system auto-assigns a unique ID number that helps to identify the type of data in the record. You can use the ID number to search for or filter the item you want to work on.

### Roles in Third-party Risk Management

Roles determine permissions and access in TPRM.

### TPRM tables that extend platform tables

TPRM has access to risk information and customer information in the same platform.

### TPRM and the Explicit Roles plugin

Activating the Third-party Risk Management plugin also installs the Explicit Roles plugin. Administrators assign the snc_internal and snc_external roles to provide internal and external users access to the instance.

### Vendor Risk Overview reports — Legacy view

The Vendor Risk Overview page is replaced by the third-party risk reports on the Vendor Management Workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Terminology

Learn more about the key concepts and terms that are used in the TPRM application.

### Third, Fourth, and nth parties

A third party is any organization or individual that you've interacted or entered into a business relationship with. Third parties can have subsidiaries and can contract with fourth parties. For example, departments are subsidiaries. A fourth party can contract with further parties (referred to as nth parties—fifth, sixth, and so on). All downstream parties (fourth through nth parties) carry risk in the same ways as third parties.

A vendor provides the goods or services that you use to produce or deliver your own goods or services. All vendors are third parties, but not all third parties are vendors. Here's a list of some other types of third parties:

- Suppliers
- Affiliates
- Counterparties
- Consultants
- Partners
- Professional services
- Advisers
- Franchises
- Dealers
- Resellers
- Distributors
- Customers
- Clients
- Outsourced staff

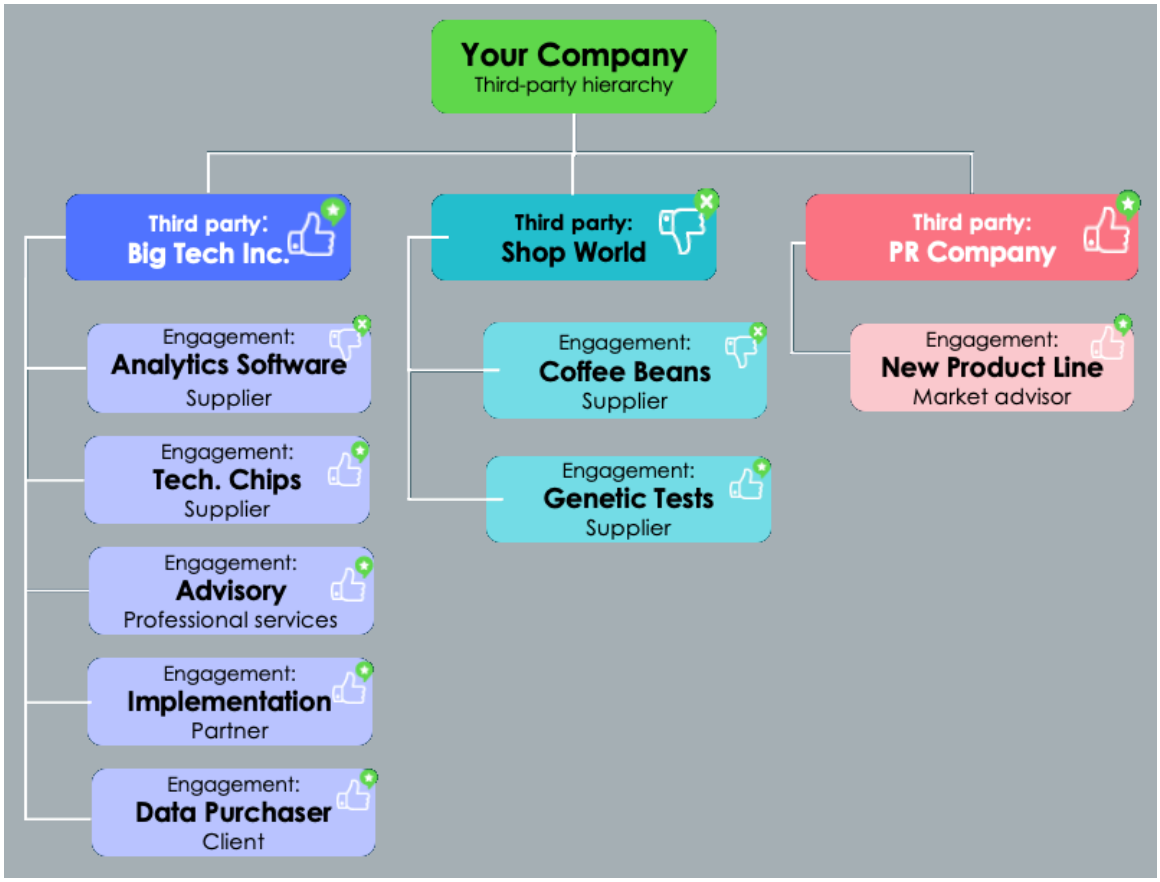
### Engagements

An engagement is the informal or contracted relationship that you intend to form with a third party that could potentially expose your organization to risk. The engagement outlines the services or products to be provided by the third party and other details of the relationship. These details can include the terms of payment, confidentiality requirements, and the duration of the relationship.

In this example, Your Company interacts with three third parties and manages several engagements among them.

In this example, Your Company interacts with 3 third parties and manages several engagements among them.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The particular third-party engagements that you might have depend on your industry, size, and operational requirements. Each engagement brings its own set of risks and requires appropriate risk management measures (due diligence) to protect your interests.

- For a detailed discussion and an example, see Why you might have several engagements with a single third party.
- For a list of the kinds of engagements that you might perform, see Types of engagement with third parties.

## IRQ—the Inherent Risk Questionnaire

During the internal risk assessment process, internal employees in your organization answer questions in the IRQ. These responses help with assessing the inherent risk that is associated with engaging with a third party. An inherent risk refers to the level of risk before implementing any risk mitigation measures. An IRQ supports the following activities:

Determining risk factors

- The nature of the services provided by the third party.
- The sensitivity of the data involved.
- The geographic location of the third party.
- The overall security posture of the third party.

Determining scoring or rating

Responses to the questionnaire are often scored or rated to help quantify the inherent risk that is associated with the third party. This scoring system can aid in prioritizing risk management efforts.

Decision making

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The results of the IRQ are then used in the decision-making process. Third-party Risk (TPR) administrators and managers can configure IRQs to send out specific external assessment (due diligence) questionnaires to the third parties based on the specific responses to questions.

- Should you engage with the third party?
- What level of due diligence is required?
- What specific risk mitigation measures should you implement?

Ongoing due diligence

The IRQ may also be part of ongoing management, with periodic reassessments to account for changes in the third party's operations, security practices, or other relevant factors.

## Due diligence (DD)

Due diligence is the process of conducting a thorough investigation or examination of the integrity, reputation, financial stability, legal compliance, operation capabilities, supply chain, and other relevant factors of a potential business partner, supplier, or vendor. Conducting due diligence on third parties is a crucial component of your comprehensive third-party risk program. You conduct due diligence to become aware of the risks that are associated with a third party so that you can confidently decide how to form your relationship.

See Why you conduct due diligence and Types of due diligence.

## Risk intelligence providers

Risk intelligence providers generate risk scores for a variety of third-party risk domains. Your organization can purchase services from providers that return data that is analogous to personal credit scores. The scores provide insight on how trustworthy and safe a particular third party can be.

See Integrating scores from risk intelligence providers.

## Due diligence request process management

From the Details tab, you can view and adjust the due diligence request information. You can also log external-facing comments and private work notes, attach files, and track request updates in the activity stream.

The **Details** tab for a due diligence request displays information in the following sections:

## Third-party due diligence request

**Third-party due diligence request**

| Field | Description |
|---|---|
| Number | For each due diligence request, the system auto-assigns a unique ID number that starts with the text **DDR**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Third-party due diligence request (continued)**

| Field | Description |
|---|---|
| State | Current state in the due diligence process: IRQ, external due diligence, approval, contract risk, or closed. |
| Request Type | • **Onboard a new engagement.** Start the onboarding process for a new engagement with an existing third party.<br>• **Reassess an existing engagement.** Reassess an existing engagement when the conditions change. For example, let's say that you hear adverse news or have changes in your third-party's supply lines. You might want to reassess the risk by conducting additional due diligence.<br>• **Reassess an existing engagement for contract renewal.** Reassess the risk before your organization renews the contract with a current third party or engagement by conducting due diligence.<br>• **Offboard an engagement with due diligence.** Determine if offboarding (terminating the relationship) with an engagement is the optimal course of action by conducting due diligence. For example, it might be too risky to switch third parties or engagements even if their current performance doesn't meet expectations.<br>• **Offboard an engagement with NO due diligence.**Request that an engagement be permanently terminated when an engagement ends or you want to switch to a different third party for other reasons. In this case, you typically don't need to conduct additional due diligence. The process does, however, include the normal Inherent Risk Questionnaire (IRQ) process to confirm that the services provided by the engagement will no longer continue. |
| Priority | Priority of the request.<br>• **1 - Critical**<br>• **2- High**<br>• **3 - Moderate** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Third-party due diligence request (continued)**

| Field | Description |
|---|---|
| | • **4 - Low**<br>• **5 - Planning** |
| Third party | Third party with which the request is associated. |
| Annual spend | Money that is spent with the third-party organization in one year. |
| Engagement | Engagement with which the request is associated. |
| Skip contract risk process | Option to skip the contract risk process.<br><br>When you select the check box, you bypass the `contract negotiation` state. The **Contract start date** and **Contract expiration date** fields are replaced with **Engagement start date** and **Engagement expiration date**. See Contract Risk process.<br><br>**Note:** After the Third-party risk (TPR) manager approves the request, it won't be sent to the contract negotiators, and the request is closed. |
| Opened by | Creator of the request. |
| Opened | Date the request was opened. |
| Contract start date, Expiration date | Preferred dates for the beginning and end of interactions with the engagement. |
| Engagement start date, Engagement expiration date | Preferred dates for the beginning and end of interactions with the engagement. |
| IRQ assessor | User at your organization that responds to the IRQ. See IRQ process management. |
| Contract negotiator | User at your organization that prepares, negotiates, and approves the contract. |
| Assignment group | Qualified group of individuals available to work on the request.<br><br>For new requests, the **Assignment group** is set to **Due diligence request assigners**. The system sends an email notification to all users in the group that is specified in the **Assignment group**. The message states that the request was received and is in the **New** state. The message also includes a link to the details page for the request.<br><br>On the due diligence request form: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Third-party due diligence request (continued)**

| Field | Description |
|---|---|
| | • Any member of the group can select **Assign to me** or set the **Owner** field to any other member of the group.<br>• A TPR manager or TPR assessor can clear the **Assignment group** field or change the value to select from different TPR assessors in the **Owner** selection list. |
| Owner | Owners are responsible for ensuring that the assessment is completed in a timely fashion by the third party, reviewing their responses, and creating and resolving issues. To drive the assessment to its completion, owners are notified when an assessment reaches a particular milestone. The owner must have the TPR manager or TPR assessor role. |
| Short description, Description | Description of the request that helps others to understand the creator's intent and requirements. |

## Third-party basic information

**Third-party basic information**

| Field | Description |
|---|---|
| Third-party name | Name of third party with which the request is associated. |
| DUNS number | Unique numeric identifier for the single business entity. A DUNS number isn't legally required for a business. |
| Street, City, State/Province, ZIP/Postal code, Country, Phone, Fax | Standard contact information for the third-party organization. |
| Website | URL for the third party. |
| Type | Type of third party. |
| Industry | The industry in which the third party is involved. |
| First name, Last name, Title, Email, Phone | Standard contact information for the third-party contact. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Engagement basic information

### Engagement basic information

| Field | Description |
|---|---|
| Engagement name | Name of engagement with which the request is associated. |
| Type | Type of product or service for this engagement. |
| Use the corporation address | Option to use the same corporation address as the third party.<br><br>When you select the check box, auto-populate the related fields with the third-party organization contact information. |
| Street, City, State/Province, ZIP/Postal code, Country, Phone, Fax | Standard contact information for the engagement organization. |
| Use the same contact | Option to use the same contact information as the third party.<br><br>When you select the check box, the related fields are auto-populated with the third-party contact information. |
| First name, Last name, Title, Email, Phone | Standard contact information for the engagement contact who will respond to the questionnaires. |

## Risk ratings

Fields are auto-populated by the current stage of the IRQ process for the request.

| Field | Description |
|---|---|
| Inherent assessment rating | Rating determined by the IRQ process. |
| Risk intelligence rating | Rating determined by data from a risk intelligence service provider. |
| Third-party assessment rating | Rating determined by responses during the external assessment process. |
| Engagement rating | Rating determined for the engagement. |

## Progress summary

Status of the due diligence processes. The fields are auto-populated by the current stage of the IRQ process for the request.

- Inherent risk assessment
- Third-party risk assessment
- Engagement risk assessment

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Compose, Activity, Attachments

The **Compose section** on the **Details** tab enables you to permanently add text to the record. The Activity section is updated with any actions on issues and tasks, submissions to TP contacts, and also with work notes and comments that users add to the record. Add text in the following fields as needed:

- **Work notes (Private)**: Information about the third-party risk assessment. Work notes are visible only to internal users who are assigned to the process.
- **Comments**: Comments about the third-party risk assessment are visible both to internal users and to third-party contacts.

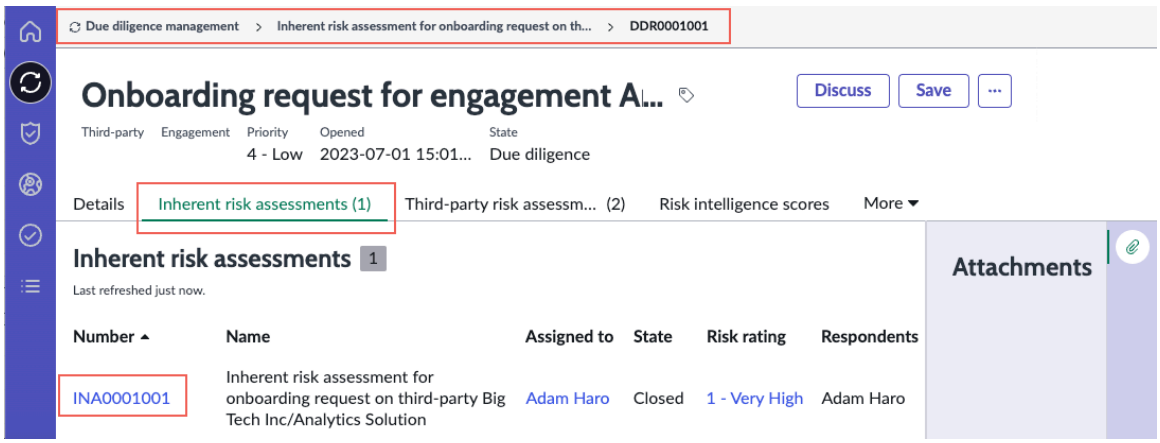
## IRQ process management

The first internal step after an engagement request is approved is to start the IRQ process to scope the risk by determining the third party's risk score.

## Accessing the IRQ process

On the Due diligence management page, select the **DDR** number for any due diligence request and then the select the **Inherent risk assessments** tab.

The tab displays the list of all IRQ processes for the engagement request. For each IRQ process, the system auto-assigns a unique ID number that starts with the text **INA**.




## Viewing the list of internal risk assessments

Inherent risk assessments tab

**Inherent risk assessments tab**

| Column | Description |
|---|---|
| Number | For each IRQ process, the system auto-assigns a unique ID number that starts with the text **INA**.<br><br>Select an INA number to work on the Third-party risk assessments page to the **Risk overview** tab.<br><br>The unique ID is used in all references to the item. You can use the ID to |

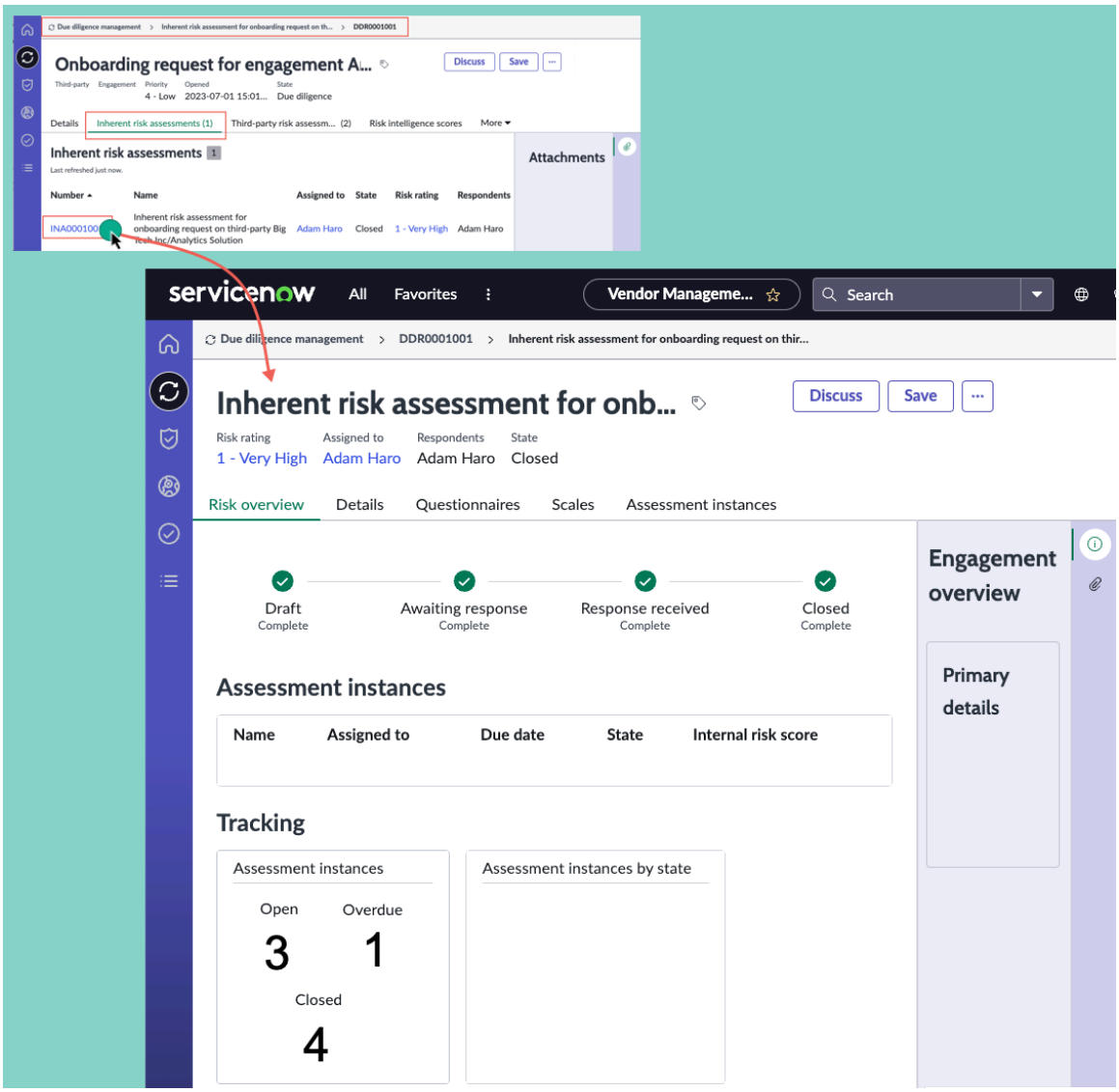
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Inherent risk assessments tab (continued)**

| Column | Description |
|---|---|
| | search or filter for the item that you want to work on. |
| Name, Assigned to, Risk rating | Data from the engagement request. |
| State | The current process in the due diligence workflow: IRQ, external due diligence, approval, contract risk, or closed. |
| Respondents | Users who responded to the request. |

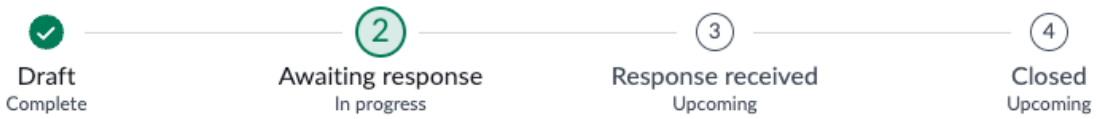
Risk overview tab on the Inherent risk assessments page

For each IRQ process, the system auto-assigns a unique ID number that starts with the text **INA**. select an INA number to work on the IRQ process on the Inherent risk assessments page.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- The symbols indicate the state of each stage in the IRQ process for the request.




- **Assessment instances** section: List of assessments that are associated with the third party.
- **Tracking** section: Count of assessments associated with the third party that are in the **Open**, **Overdue**, and **Closed** status.

Details tab on the Inherent risk assessments page

- **Internal assessment section**: General information on the third party plus schedules for the overall assessment and questionnaire due dates from the engagement due diligence request.

- The **Compose section** on the **Details** tab enables you to permanently add text to the record. The Activity section is updated with any actions on issues and tasks, submissions to TP contacts, and also with work notes and comments that users add to the record. Add text in the following fields as needed:
  - **Work notes (Private)**: Information about the third-party risk assessment. Work notes are visible only to internal users who are assigned to the process.
  - **Comments**: Comments about the third-party risk assessment are visible both to internal users and to third-party contacts.
- The **Third-party overview** section provides key information on the third party that is associated with the engagement request.

Questionnaires tab on the Inherent risk assessments page

The tab lists all open IRQs. Select a name to view the details.

Scales tab on the Inherent risk assessments page

The tab lists the definitions of the calculated rating and tier values. See Set up risk rating scales and scoring and Third-party risk tiering assessments — Legacy process for instructions for defining the settings.

Assessment instances tab on the Inherent risk assessments page

All values on the tab come from the internal assessments that have been conducted on the third part in the engagement.

**Assessment instances tab**

| Column | Description |
|---|---|
| Number | For each IRQ process, the system auto-assigns a unique ID number that starts with the text **INA**.<br><br>The unique ID is used in all references to the item. You can use the ID to |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Assessment instances tab (continued)**

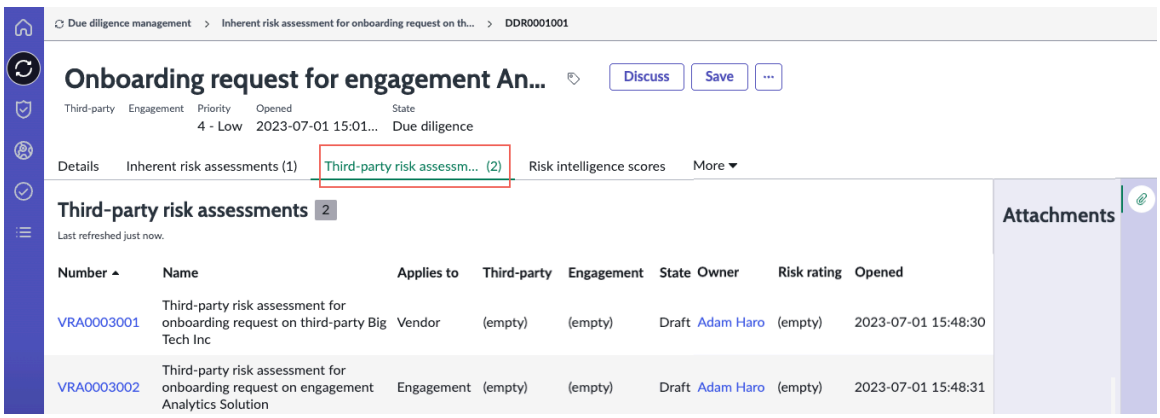
| Column | Description |
|---|---|
| | search or filter for the item that you want to work on. |
| Metric type | Questionnaire that determined the questionnaires used in the assessment. |
| Assigned to | User that is responsible for managing and responding to the IRQ. |
| Due date | Deadline for third party to respond to and return all questionnaires. |
| State | Current stage of the IRQ process for the engagement request. |
| Internal risk score | An engagement risk-scoring rule specifies component criteria that determine which engagements are selected for assessment. For example, a rule could enable assessments for engagements that involve more than $40,000 annual business. Engagement scoring rules apply only to engagements.<br><br>See Define engagement risk scoring rules. |

## Third-party (external) risk assessment management

After the IRQ process is complete, you send questionnaires and document requests to the third-party contact. You manage the third-party risk assessment by working with the contacts to help ensure that the responses are complete and accurate.

## Accessing an external risk assessment

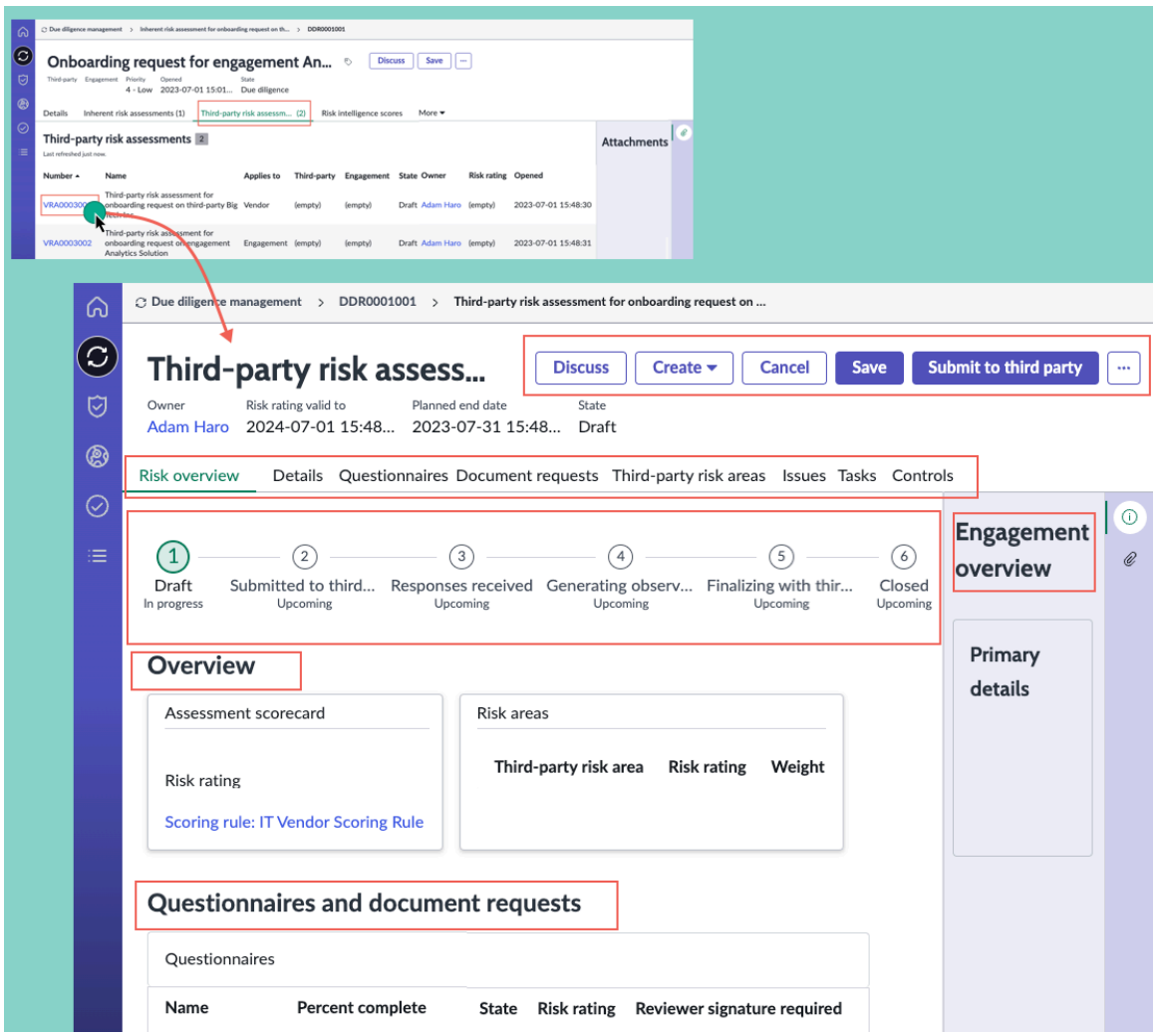
On the Due diligence management page, select the **DDR** number for any engagement due diligence request and the select the **Third-party risk assessments** tab. The tab displays the list of all third-party risk assessments (external due diligence processes) for the selected engagement request.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Working on a third-party risk assessment

For each external risk assessment, the system auto-assigns a unique ID number that starts with the text **VRA**. A risk assessment can represent the work on an engagement request for a third-party organization or an engagement request for a group within the parent organization. Select a VRA number to work on the risk assessment on the **Third-party risk assessments** tab.




## Actions on any tab

### Actions

| Action | Description |
|---|---|
| Discuss | Select **Discuss** to send a message to other users. The message is recorded in the **Activity** section of the **Details** tab. |
| Create | Create an issue or task as describe in the following sections. |
| Save | Select **Save** to save any change you made to a value on any tab. |
| Submit to third party | Submit all questionnaires and document requests to the TP contact. The action is |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

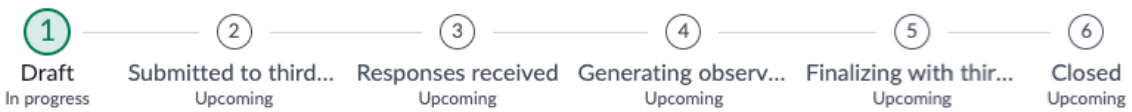
**Actions (continued)**

| Action | Description |
|---|---|
| | recorded in the Activity section on the **Details** tab. |
| … Delete | Select **Delete** to delete the record of the engagement request. |
| Adding an attachment | Select **Browse** in the **Attachments** section or select the attachment icon to select and add an attachment. |

## Working on third-party risk assessments

Risk overview tab on the Third-party risk assessments page

- The symbols indicate the current state of the external risk assessment process for the engagement request. See Life cycle states of a third-party (external) risk assessment for descriptions of the states.




- **Overview** section: List of assessments that are associated with the engagement.
- **Questionnaires and document requests** section: List of questionnaires and document requests for the engagement.
- **Fourth-nth party questionnaires** section: List of questionnaires and document requests for fourth parties and their sub-parties that are associated with the engagement.
- **Tracking** section: Count of assessments associated with the third party that are in the **Open**, **Overdue**, and **Closed** status.

Details tab on the Third-party risk assessments page

- Third-party risk assessment section: General information on the third party plus schedules for the overall assessment and questionnaire due dates from the engagement due diligence request.

- The **Compose section** on the **Details** tab enables you to permanently add text to the record. The Activity section is updated with any actions on issues and tasks, submissions to TP contacts, and also with work notes and comments that users add to the record. Add text in the following fields as needed:
  - **Work notes (Private)**: Information about the third-party risk assessment. Work notes are visible only to internal users who are assigned to the process.
  - **Comments**: Comments about the third-party risk assessment are visible both to internal users and to third-party contacts.

Questionnaires tab on the Third-party risk assessments page

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The tab lists the questionnaires that the third-party contact will respond to. Select a name to view the details. See Create and configure an external questionnaire.

To enable TPR assessors to modify responses, configure the **Allow TPR assessors to modify responses in third-party questionnaires** [`sn_svdp.allow_assessor_edit`] system property. You can set the following options:

- Enable TPR assessors to answer questions or modify responses (default)
- Enable TPR assessors to modify responses
- Do not enable TPR assessors to answer questions or modify responses

See Configure TPRM properties.

Document requests tab on the Third-party risk assessments page

The tab lists the requests for documents that the third-party contact should return. The information in the columns helps you to prioritize your work in following up with third-party contact. In particular, the state and percent complete values are key indicators. Select a name to view the details. See Create a document request template.

Third-party risk areas tab on the Third-party risk assessments page

A risk domain defines the type of risk to assess for a third party. For example, you might want to assess a data-management third party in terms of security risk and a bank in terms of financial risk. Security risk and financial risk are risk domains. Some platform applications refer to risk domains as "risk areas." See Define a third-party risk domain.

Issues tab on the Third-party risk assessments page

In an iterative process, before the TPR manager closes an assessment, the TPR manager can generate non-compliance issues and tasks. The TPR manager communicates with the TP contacts by using comments to close the issues and tasks. The TPR manager can also assign different TP contacts as needed. See Create an issue for a third party or engagement and Manage issues.

Tasks tab on the Third-party risk assessments page

In an iterative process, before the TPR manager closes an assessment, the TPR manager can generate non-compliance issues and tasks. The TPR manager communicates with the TP contacts by using comments to close the issues and tasks. The TPR manager can also assign different TP contacts as needed. See Create a task for a third party or engagement and Manage a task for a third party or engagement.

Related topics

Life cycle states of a third-party (external) risk assessment

Define a third-party risk domain

Manage issues

Manage a task for a third party or engagement

## Request third-party risk due diligence request form

The due diligence request form captures all the initial information that you need to start the due diligence process. Any employee within your organization can request due diligence. If you're selecting an existing third party, a significant portion of the information is automatically filled in.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Request third-party risk due diligence form

| Field | Description |
|---|---|
| **Third-party information section** | |
| Name, DUNS number, Phone, Industry, Website, and Fax | Standard information for the parent organization.<br><br>A DUNS number isn't legally required for a business.<br><br>**Note:** The third party that you identify here might be the target of your engagement request, or it might be the parent of the new engagement. You add the information about the engagement organization in the following Engagement information section. |
| **Engagement information section** | |
| Name | Name that identifies this engagement on all forms and lists. |
| Type | Type of product or service that the engaged organization provides. |
| Phone / Fax | Phone and fax numbers of the department or subsidiary organization that the engagement relates to. This number could differ from the number for the parent third party. |
| Request start date | Date by which you need the engagement to be active so that you can engage with the third party. This information helps the Third-party risk (TPR) manager to prioritize your request. |
| Request end date | Date at which you expect to end the engagement. |
| User who will respond to the initial IRQ | Person with the IRQ assessor role who should respond to the IRQ. For more information, see Respond to an Inherent Risk Questionnaire (IRQ).<br><br>**Note:** While reviewing this request for due diligence, the TPR manager or owner can specify a different user. |
| **Third-party address section** | |
| Street, City, State/ Province, ZIP/ Postal code, Country | Standard address information for the parent organization.<br><br>**Note:** The third party that you identify here might be the target of your request, or it might be the parent of the organization that you engage with. You add the information about the engagement organization in the following Engagement address section. |
| **Engagement address section** | |
| Street, City, State/ Province, ZIP/ Postal code, Country | Standard address information for the engagement organization.<br><br>Select **Same as third-party address** if the target of your engagement request is the parent third-party organization. |
| **Third-party primary contact section** | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Request third-party risk due diligence form (continued)**

| Field | Description |
|---|---|
| First name, Last name, Title, Email, and Phone | Standard contact information for the person at the third-party organization who acts as the primary third-party contact.<br><br>For a description of the responsibilities of the third-party contact role, see Roles in Third-party Risk Management. |
| **Engagement primary contact section** | |
| First name, Last name, Title, Email, and Phone | Standard contact information for the person at the engagement organization who acts as the primary third-party contact.<br><br>If the target of your engagement request is the parent third-party organization, select **Same as third-party primary contact**.<br><br>For a description of the responsibilities of the third-party contact role, see Roles in Third-party Risk Management. |

Related topics

Requesting third-party risk due diligence

Request due diligence for a third-party engagement

## Domain separation and Third-party Risk Management

Domain separation is supported for TPRM. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

## Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

For more information on support levels, see Application support for domain separation.

## Overview

The ServiceNow® GRC: Third-party Risk Management (TPRM) application enables you to proactively identify, assess, and mitigate risks that are associated with your third-party relationships. TPRM provides a centralized process for managing your portfolio of third parties, assessing and scoring risk, and performing remediation. TPRM supports domain separation at the basic level (level 0 or data level). Your Managed Service Provider can configure TPRM at the process level of domain separation.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## How domain separation works in TPRM

- All TPRM tables support the data level of domain separation. No special setup is needed except for adding the domain-related columns to form views or list views.
- When TPRM is installed to an instance where domain separation is activated, all TPRM data is automatically domain-separated. See the platform domain separation documentation for details.

## Use cases

Tenant domains manage their own application data in the same way as data is managed on an instance.

## Domain-separated tables

There is no **Domain** column in TPRM application tables.

All TPRM tables support data-level domain separation with sys_domain and sys_domain_path columns.

Related topics

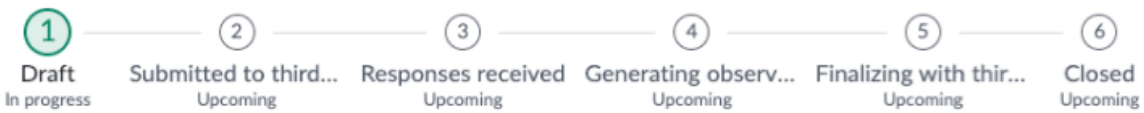
Domain separation for service providers

## Life cycle states of a third-party (external) risk assessment

The process of collecting assessment data from a third party moves between several states. For example, during the **Submitted to third party** state, the third party responds to tasks, issues, and works to complete the questionnaires.

## Third-party assessment states

**Third-party assessment states**




Draft

An external assessment record is opened in the **Draft** state.

- **Assessment template:** A set of external questionnaires and document requests that are auto-generated based on IRQ responses. Alternatively, an administrator could manually specify the questionnaires and document requests.
- **Risk rating:** The overall risk rating that is auto-generated based on IRQ responses.
- **Owner:** The owner is the person who owns an assessment for audit purposes and monitors and manages overall assessment processes. Owners are responsible for confirming that the assessment is completed in a timely fashion by the third party, reviewing their responses, and creating and resolving issues. To drive the assessment to its completion, owners are notified when an assessment reaches a particular milestone. The owner must have the TPR manager or TPR assessor role.

Submitted to third party

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The questionnaires and document requests for the assessment have been sent to the third-party contact. Internal stakeholders await responses.

Responses received

After contacts at the third party have completed all questionnaires and document requests, your internal third-party risk team reviews and analyzes the responses. The team might return particular questions for follow-up, clarification, or missing answers.

Generating observations

When all responses are completed, the system can auto-generate issues for incorrect answers.

Third-party contacts respond to issues. Your internal third-party risk team makes a final determination to accept the responses or remediate the issues.

Finalizing with a third party

Your third-party risk team reviews all assessment data. In some cases, the team resets the assessment to the **Draft** state to restart the assessment life cycle.

Closed

When all data is acceptable, the assessment is complete and a member of the team closes the assessment. If the engagement will be contracted, the **Closed** state initiates the contract risk process.

## Third-party risk ratings and scoring calculations

Perform a comprehensive external risk assessment when calculating multiple ratings and scores by using the Third-party Risk Management application. You can gain a deeper understanding of the overall calculation process and learn how user-defined parameters and configurations influence the results of the questionnaires.

## Risk rating scale

Every time that you create a questionnaire, the system applies a default risk rating. You can configure the risk rating scale, which includes the categories, minimum, and maximum values, to meet your specific questionnaire needs that can vary for each assessment. For example, you can define risk rating values as colors rather than **1-Very High** through **5-Very Low**.

The following example shows the default risk ratings that are provided as part of the base system.

**Default risk rating scale**

Default Risk Rating Scales View: Third-party risk New

| Risk rating | Order ▲ | Minimum | Maximum |
|---|---|---|---|
| 1 - Very High | 1 | 0 | 19 |
| 2 - High | 2 | 20 | 39 |
| 3 - Moderate | 3 | 40 | 59 |
| 4 - Low | 4 | 60 | 79 |
| 5 - Very Low | 5 | 80 | 100 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Score calculation mechanism

The score calculation mechanism for each external risk assessment uses the Now Platform® assessment score calculation engine. This engine performs these calculations by using a series of related equations that are dynamically recalculated. You define the following parameters that affect the calculated assessment rating:

- Questions (metrics)

  For more information on how to define a question, see Define a question.

- Metric scale definition

  For more information on how to define the metric scale definition, see Define a question.

- Categories

  For more information on how to define a category, see Set up and maintain a question bank.

- Weights

  For more information on how to define a weight, see Define component criteria.

- Risk rating scale

  For more information on how to define a risk rating scale, see Set up risk rating scales and scoring.

- Business service rating scale

  At the end of the scoring calculation, if a third party or engagement is associated with a business service that you defined in the Service [cmdb_ci_service] table, that criticality weight is factored into the calculation. Different business services may have varying levels of associated risks. By adjusting the criticality weight, you can use the resulting values to adjust your risk mitigation strategies.

  **Note:** A business service is a defined sequence of tasks or activities that contribute to the delivery of a service such as email, IT services, E-commerce.

  You can define the criticality weights by navigating to **All** > **Self-Service** > **Third-party Risk Management** > **Assessment Setup** > **Business Service Rating Scale**.

  As part of the base system, four ratings are defined:

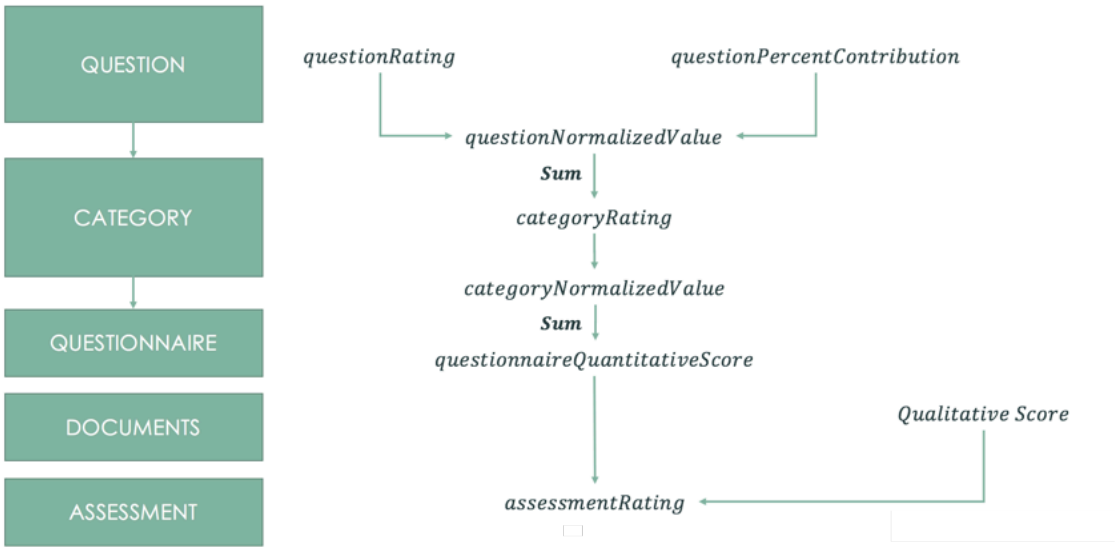
  - 1 - most critical
  - 2 - somewhat critical
  - 3 - less critical
  - 4 - not critical

  You can associate each third party or engagement with multiple business services.

The following infographic shows the assessment rating calculation process.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Assessment rating calculation process




1. Each question on the questionnaire has these values calculated:
   a. questionRatings: The rating for each question is calculated by the responses. The rating is determined by the metric scale definition and the values that are associated with the answers.
   b. questionPercentContribution: The percent contribution of each question within its category is determined by this calculation. This value is based on the weight that is assigned by the third-party risk manager to the question and the overall weight of the category.
   c. questionNormalizedValue: The normalized value for each question is calculated by multiplying the question rating, question percent contribution, and a constant value (100). This value enables you to compare questions with different weights and ratings.
2. The categories of each questionnaire has these ratings calculated:
   a. categoryRating: The rating for each category is calculated by summing up the normalized values of all the questions within the category. The category rating is derived from the associated risk rating scale.
   b. categoryNormalizedValue: The category rating is normalized by multiplying it with the category weight to enable you to compare values across all categories.
3. Questionnaire, questionnaireQuantitativeScore: The overall quantitative score for the assessment is calculated by summing up the normalized category scores. This score represents the risk score for the questionnaire.
4. Documents, Qualitative Score: The calculation for the qualitative risk rating for the document requests is based on the answer to the default question "Do you have document 'document name'? on the document request. This rating can be overridden by the third-party risk assessor if necessary.
5. Assessment, assessmentRating: The final rating for the assessment is calculated by taking the weighted average of the questionnaires and document requests within each third-party risk area. The weights are determined by the risk area scoring method.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

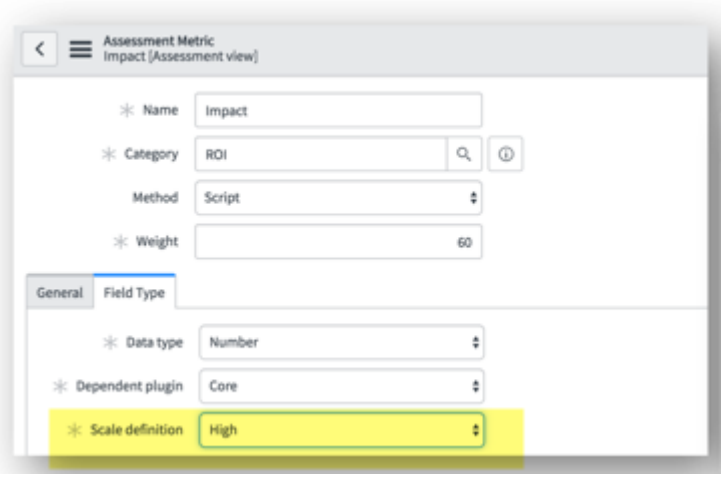
## questionRating calculation

You use the `questionRating` calculation to define the relative degree of significance of each individual assessment metric as compared to other metrics. This key variable helps to calculate the normalized value later in the process.

You can define the **Scale definition** for an individual assessment metric by setting it to be **High** or **Low**.

The following example shows how the metric scale definition field was defined in the Assessment Metric form.

### Metric scale definition example




- **High** means that large numerical values indicate a positive result. If the metric scale definition is high, the following equation is used:

```
questionRating = (value - minValue) / (maxValue - minValue)
```

- **Low** means that small numerical values indicate a positive result. If the metric scale definition is low, the following equation is used:

```
questionRating = 1 - ((value - minValue) / (maxValue - minValue))
```

The following example shows the question value field that is defined in the assessment instance question form.

### Assessment question value example




The **value** used in the equation is taken from the response to the question. The configuration of the metric defines the correct answer, which is the value, and the other values that are associated with the other incorrect or less desirable answers.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## questionPercentContribution calculation

The `questionPercentContribution` defines the degree of significance of the assessment metric within the category where it's included. This key variable is used in calculating the normalized value later in the process.

The following equation is used to calculate the `questionPercentContribution`.

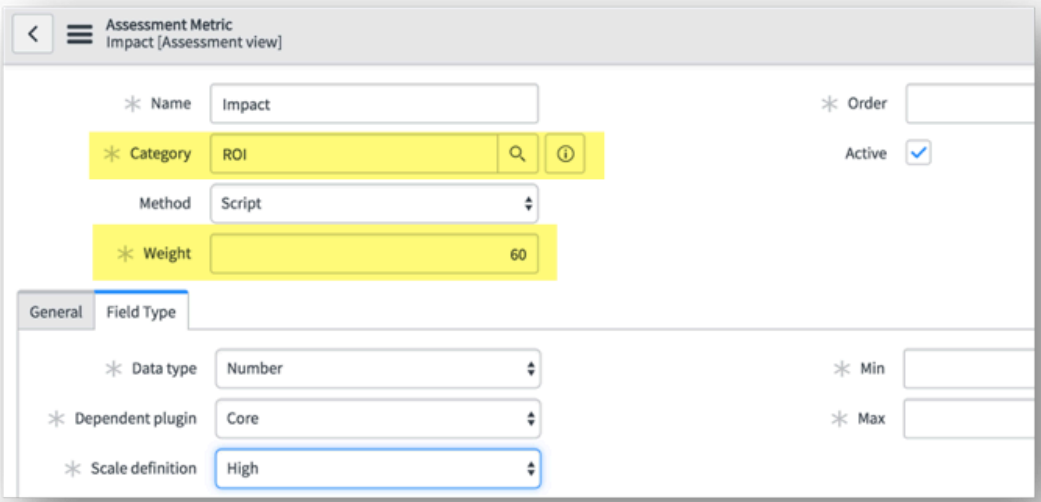
```
questionPercentContribution = (questionWeight /
sumOfAllQuestionWeightsWithinCategory)
```

The **Category** represents a theme for evaluating the assessable records in a metric type. You can define this category's example with the return on investment (ROI), risk, performance, security, personal data, and so on.

The **Weight** is a numerical value that represents the metric importance that relates to other metrics. A higher weight in proportion to the overall weight of the category has a stronger influence on the final score. You can define the weight, set it to any integer, and apply it to questions and categories.

The following example shows the question category and weight field that you can define in the assessment metric form.

### Assessment question category and weight example




## questionNormalizedValue calculation

The `questionNormalizedValue` enables questions with different weights and ratings to be compared equally on the same scale.

The following equation is used to calculate the `questionNormalizedValue`.

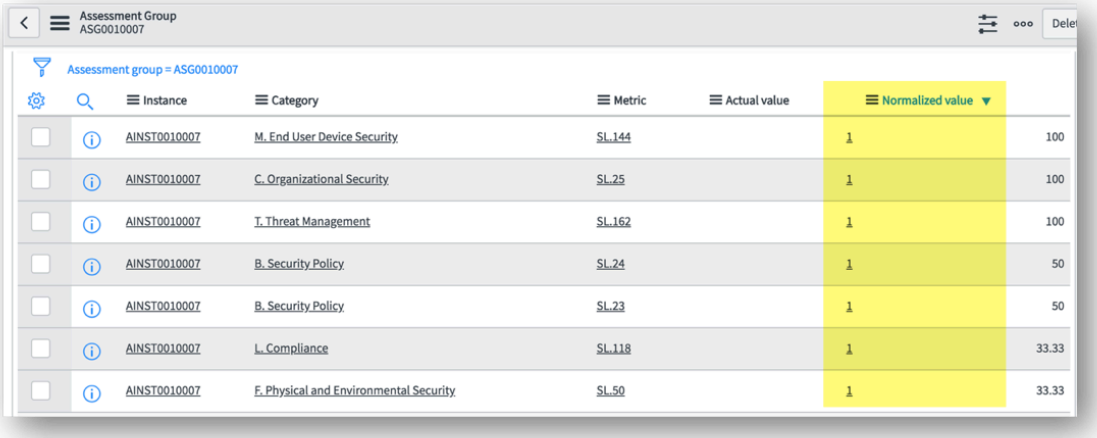
```
questionNormalizedValue = 100 * questionRating *
questionPercentContribution
```

Each answer to every question (assessment metric) on the questionnaire has a **normalized value**. This normalized value enables you to make a meaningful comparison that is later rolled up to the category and the overall assessment results.

The following example shows a list of normalized values for an assessment group.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Normalized value list for an assessment group example




## categoryRating calculation

Now that there are normalized values for each metric within the category, the `categoryRating` calculates a value for the entire category that can then be normalized by using the `categoryNormalizedValue` equation to facilitate inter-category comparisons.

The following equation is used to calculate the `questionPercentContribution`.

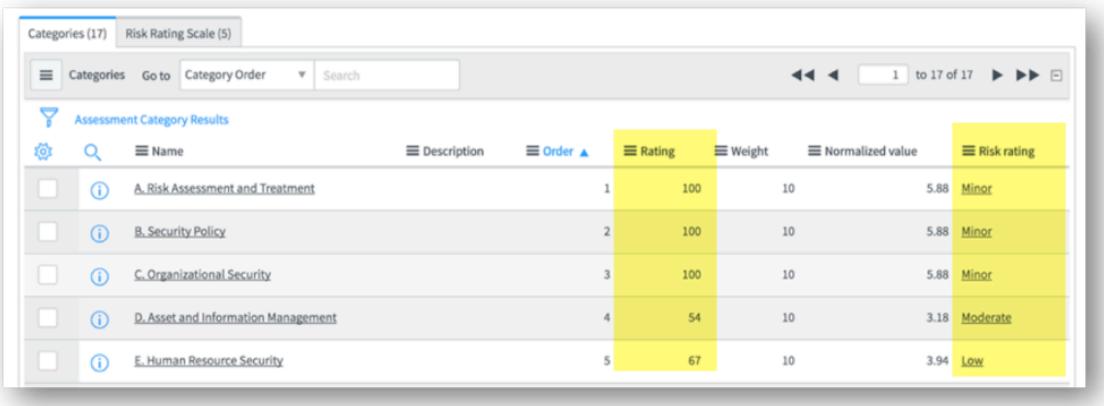
```
categoryRating = sumOfAllQuestionNormalizedValuesWithinCategory
```

The category **Rating** is the sum of all normalized values for the metrics within the category.

The stated **Risk Rating** for each category is derived from the associated Risk Rating Scale.

The following example shows the list of category ratings and risk ratings for an assessment category.

### Categories rating and risk rating list example




## categoryNormalizedValue calculation

With the Category Ratings established, the `categoryNormalizedValue` equation uses this rating and the category weight to normalize the result across all categories.

The following equation is used to calculate the `categoryNormalizedValue`.

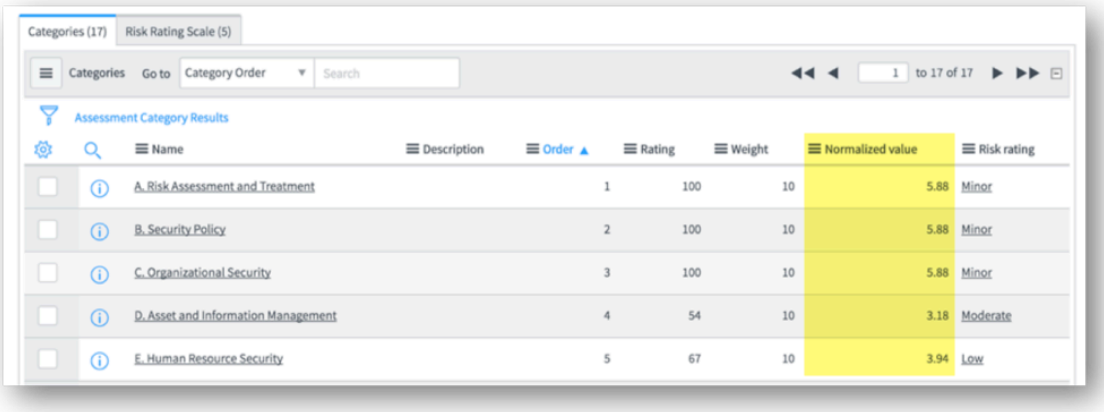
```
categoryNormalizedValue = categoryRating * (categoryWeight /
sumOfAllCategoryWeights)
```

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This calculated normalized value performs a more meaningful comparison that is later rolled up to the overall assessment results. Higher **categoryWeight** values increase the normalized value of the category.

The following example shows the list of normalized values for an assessment category.

### Categories normalized value list example




## questionnaireQuantitativeScore calculation

With all categories normalized, the overall quantitative score for the assessment is calculated.

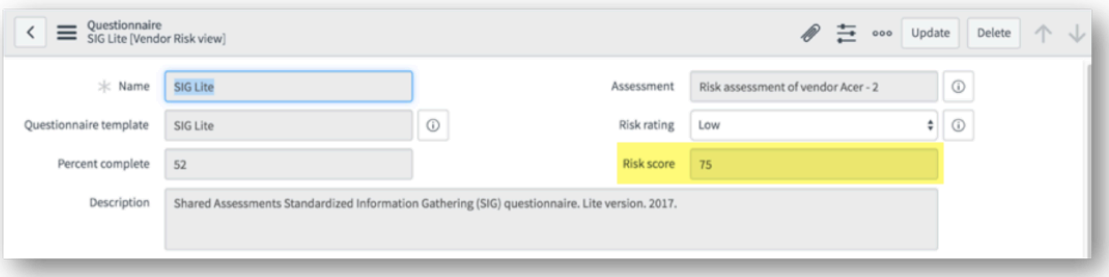
The following equation is used to calculate the `questionnaireQuantitativeScore`.

```
questionnaireQuantitativeScore = sumOfAllCategoryNormalizedValues
```

The output from the `questionnaireQuantitativeScore` equation is the sum of the normalized category scores. It's presented as the **Risk Score** on the record for the questionnaire.

The following example shows a risk score for a questionnaire.

### Questionnaire record with risk score example




## Qualitative score for documents

Document Requests have a risk rating that is a qualitative score. The preliminary risk rating is based on the answer to the default question "Do you have document 'document name'?".

The document risk rating uses the scale that is shown in the following table.

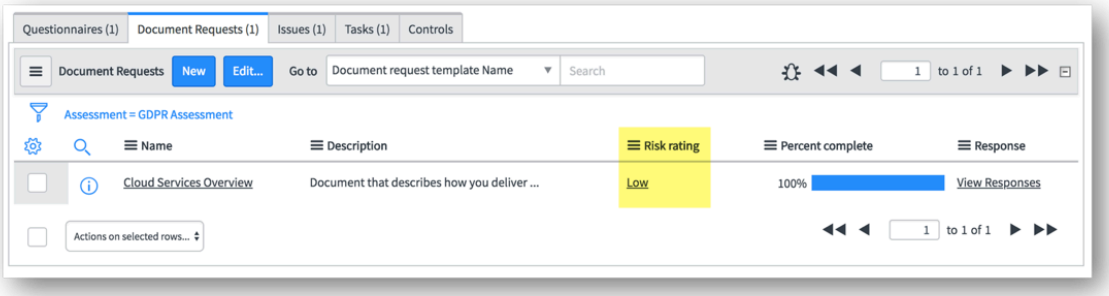
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Document risk rating scale

| Response | Risk Rating |
|---|---|
| Yes | Low |
| No or unanswered | High |
| N/A | Moderate |

The following example shows a risk rating for a document request.

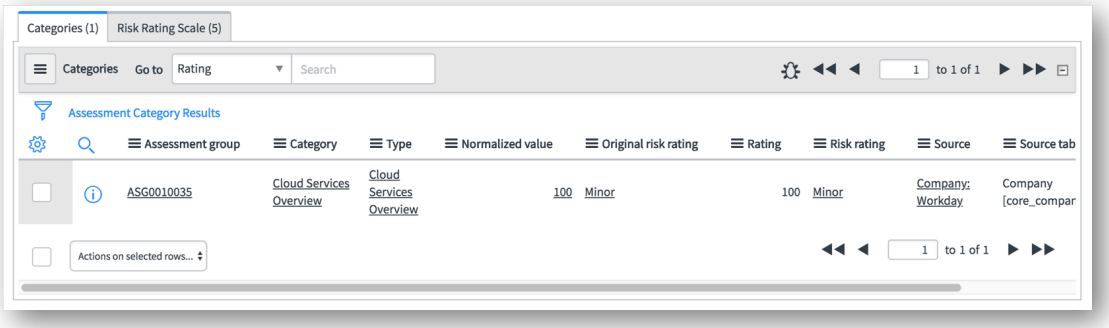
#### Document request risk rating example




After the document is reviewed, it might be found to be deficient, so the Third-party risk assessor can override the default rating. The assessment retains the current **Risk Rating** and the **Original Risk Rating**. The stated **Risk Rating** for each category is derived from the associated Risk Rating Scale.

The following example shows a categories related list that includes the original and current risk rating.

#### Categories related list example




## assessmentRating calculation

For any external risk assessment, the final rating for the assessment is calculated as the weighted average of the questionnaires and document requests within each third-party risk area.

The following equation is used to calculate the `assessmentRating`.

```
assessmentRating = (AVG (Questionnaire + Document Request for a risk area) * weight assigned to that risk area + (Questionnaire + Document Request for another risk area) * weight assigned to that risk area) / the sum of the weights
```

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Questionnaire 1 = defined in the Security Risk Area
- Questionnaire 2 = defined in the Financial Risk Area
- Questionnaire 3 = defined in the Financial Risk Area
- Document Request 1 = defined in the Security Risk Area

The risk area criteria are set like the example shown in the following table:

**Risk area criteria**

| Risk Area | Scoring Method | Weight |
|---|---|---|
| Security Risk | Average Risk | 10 |
| Financial Risk | Max Risk | 20 |

The final rating for the assessment is calculated by using this equation:

```
assessmentRating = (AVG (Questionnaire 1 + Document Request 1) * 10 + MAX (Questionnaire 2 + Questionnaire 3) * 20) / (10 + 20).
```

The final rating is the overall assessment rating that considers the scores and ratings from all assessments conducted for a third-party or engagement. It's calculated by taking the weighted average of the questionnaires and document requests within each risk area. This calculation process ensures that all relevant metrics, categories, and weights are taken into account based on how you defined these parameters and configurations. The calculation process and the factors involved can help you make informed decisions and take appropriate actions based on the final rating.

## Guidelines for importing spreadsheet data

Before you try to import the questionnaire data from a Microsoft Excel spreadsheet into Third-party Risk Management tables, you must verify that its format meets particular guidelines.

## Property settings that affect spreadsheet data

You can specify the following property settings:

Text delimiter in spreadsheets [`sn_vdr_risk_asmt.excel_choice_delimiter`]

Character string that separates response text in questions of type 'Choice' and 'Multiple Selection'.

Common delimiters: \r, \n, \t, \r\n, and the comma character.

Maximum spreadsheet file size [`sn_vdr_risk_asmt.excel_file_max_size`]

Maximum file size in MB that can be imported.

See Configure TPRM properties.

## Supported columns

Required columns are marked with *. Column headings must appear in the first row of the spreadsheet.

- Serial number *
- Category *
- Question *

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Order *
- Data type *
- Description
- Scored
- Correct answer
- Scale definition
- Depends on
- Displayed when
- Min
- Max
- Weight
- Mandatory
- Allow additional information
- Allow not applicable
- All other columns of the Assessment Metric [asmt_metric] table

### Supported question types

- Check box
- Yes/No
- Choice
- Attachment
- Date
- Date/Time
- Percentage
- String
- Multiple Selection
- Number
- Numeric Scale

### Supported Excel formats

Requirements:

- Each file can have only one worksheet.
- You can separate multiple choices in a cell with line breaks (Alt/Option + Enter). Other options are available in System Properties.

- .xlsx
- .xls
- .xlm
- .xltx
- .xlt

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- .xlw
- .xlsb
- .csv

Related topics

Configure TPRM properties

## Unique ID numbers for TPRM records

When you create (or the system generates) a new record (for example, a request for due diligence or a task), the system auto-assigns a unique ID number that helps to identify the type of data in the record. You can use the ID number to search for or filter the item you want to work on.

## Unique text prefixes for ID numbers that identify the type of record

- **Contracts**: For each contract, the system auto-assigns a unique ID number that starts with the text **C** or **CNTR**.
- **Controls**: For each control, the system auto-assigns a unique ID number that starts with the text **CTRL**.
- **Due diligence requests**: For each due diligence request, the system auto-assigns a unique ID number that starts with the text **DDR**.
- **Engagement risk scoring rules**: For each engagement risk scoring rule, the system auto-assigns a unique ID number that starts with the text **ERS**.
- **Event-driven management**: For each Event-driven management rule, the system auto-assigns a unique ID number that starts with the text **EMR**. In the history table of rule runs (executions), the system auto-assigns a unique ID number for each run that starts with the text **EMH**.
- **IRQs**: For each IRQ process, the system auto-assigns a unique ID number that starts with the text **INA**.
- **Issues**: For each issue, the system auto-assigns a unique ID number that starts with the text **VRI**.
- **Tasks**: For each task, the system auto-assigns a unique ID number that starts with the text **VRT**.
- **External risk assessments (the external due diligence process where third-party contacts respond to requests for information)**: For each external risk assessment, the system auto-assigns a unique ID number that starts with the text **VRA**.
- **Third-party risk scoring rule**: For each third-party risk scoring rule, the system auto-assigns a unique ID number that starts with the text **VRS**.
- **Risk tiering assessment**: For each risk tiering assessment, the system auto-assigns a unique ID number that starts with the text **VTA**.

## Roles in Third-party Risk Management

Roles determine permissions and access in TPRM.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## TPRM roles

| Friendly name [role name] | Description | Contains roles |
|---|---|---|
| Third-party reader [vendor_reader] | Read access to third-party contact records. | None |
| Third-party editor [vendor_editor] | Create/update/delete third-party contact records. | None |
| Third-party assessment reviewer<br><br>[sn_vdr_risk_asmt.vendor_assessment_reviewer] | View assessment and questionnaire data. In addition to viewing, they can leave comments on the following tables:<br>• Tiering assessment<br>• Internal assessment<br>• External risk assessment<br>• Third-party risk issues<br>• Third-party risk tasks<br>• Third-party risk due diligence request | Contains:<br>• compliance_reader<br>• risk_reader<br>• task_editor<br>• vendor_reader |
| TPR assessor (Third-party risk assessor)<br><br>[sn_vdr_risk_asmt.vendor_assessor] | • Includes all permissions of the Third-party assessment reviewer role plus: Manage third parties, third-party contacts, external risk assessments, and issues.<br>• You can set the following options for the `sn_svdp.allow_assessor_edit` property:<br>◦ Enable TPR assessors to answer questions or modify responses in third-party questionnaires (default).<br>◦ Enable TPR assessors to modify responses.<br>◦ Do not enable TPR assessors to answer questions or modify responses.<br>See Configure TPRM properties. | Contains:<br>• compliance_reader<br>• vendor_assessment_reviewer<br>• vendor_editor<br>• vendor_reader |
| TPR approver | Includes all permissions of the Third-party assessment | Contains vendor_assessment_reviewer |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Friendly name [role name] | Description | Contains roles |
|---|---|---|
| [sn_vdr_risk_asmt.approver] | reviewer role plus: approve IRQs. | |
| TPR manager (Third-party risk manager)<br><br>[sn_vdr_risk_asmt.vendor_risk_manager] | Includes all permissions of the TPR assessor role plus:<br>• Manage third-party assessment templates and scheduled assessments.<br>• Manage engagements and engagement contacts.<br>• Manage scoring rules for both third-parties and engagements. | Contains vendor_assessor |
| TPR admin (Third-party risk admin)<br><br>[sn_vdr_risk_asmt.vendor_risk_admin] | Includes all permissions of the TPR manager role plus:<br>Create and edit the following items:<br>• Third-party assessment templates<br>• Risk tiering templates<br>• Risk tier questionnaire templates<br>• Third-party questionnaire templates<br>• Document request templates<br>• Scheduled assessments | Contains<br>• vendor_risk_manager<br>• assessment_admin |
| Contract risk negotiator<br><br>[sn_vdr_risk_asmt.contract_negotiator] | Includes all permissions of the TPR assessor role plus:<br><br>Gives users in the legal department access to modify contract status and the start and expiration dates.<br><br>You can add users with this role to the **Contract risk negotiators** user group. See Add users to groups based on responsibilities. | Contains vendor_assessor |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Friendly name [role name] | Description | Contains roles |
|---|---|---|
| [vendor_contact]<br>• Called a third-party contact when responding to an external questionnaire/task/issue for a third party.<br>• Called an engagement contact when responding to a questionnaire/task/issue for an engagement. | You assign the third-party contact role to users at the third-party organization whose risk is being assessed. Third-party contacts are assigned the snc_external role to give them access to resources and actions in the Third-party portal.<br>**Important:** The third-party contact role should be used only for external contacts. The role prohibits access to your Now Platform instance and grants access only to the Third-party portal.<br>You assign the **primary contact** responsibility to the third-party contact who can directly answer assessment questions or assign another contact at the third party to answer the questions. Primary contacts can manage other contacts for the third party. | Contains snc_external |

Related topics

Assign TPRM roles to users and user groups

## TPRM tables that extend platform tables

TPRM has access to risk information and customer information in the same platform.

Access to risk information and customer information in the same platform supports the new OCC guidelines.

Tables that extend core_company

The tables that extend core_company work with the TPRM model, no matter how many extensions down.

- service_now_customer: Service-now Operations application.
- sn_bom_financial_institution: Financial Services Operations application.
- sn_customer_service_organization: Customer Service Management (CSM) application
- customer_account: Customer Service Management (CSM)

Tables that extend from sn_customer_service_organization

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_Customer Service Management (CSM)_business_location: Customer Service Management (CSM) application.
- sn_outsourced_service_provider: Customer Service Management (CSM) application.
- sn_hcls_organization: Healthcare service management (HSM) application.

Tables that extend from sn_Customer Service Management (CSM)_business_location

- sn_Customer Service Management (CSM)_business_location_internal: Customer Service Management (CSM) application
- sn_Customer Service Management (CSM)_business_location_external: Customer Service Management (CSM) application
- sn_hcls_location: Healthcare service management (HSM) application

## TPRM and the Explicit Roles plugin

Activating the Third-party Risk Management plugin also installs the Explicit Roles plugin. Administrators assign the snc_internal and snc_external roles to provide internal and external users access to the instance.

When third-party contacts are created, they are automatically assigned the snc_external role, giving them access to resources related to the Third-party portal.

Various tables provide role-based access to record by setting the **Roles** field. If the **Roles** field is empty, all users have access to that record. For example, if the **Roles** field for a Service Catalog item has an empty **Roles** field, all users have access to that Service Catalog item.

However, when the Explicit Roles plugin is installed, the **Roles** field is updated to **snc_internal**. Also, all users are given the snc_internal role. Continuing with the previous example:

- Before installing the Explicit Roles plugin, if a Service Catalog item had an empty **Roles** field, it was accessible to every user.
- After installing the Explicit roles plugin, the **Roles** field of the Service Catalog item is updated to snc_internal and all existing users are given the snc_internal role, making the catalog item accessible to those users.
- After that, all new users must be assigned the snc_internal role, or they will not have access to that Service Catalog item.

The following table describes the changes to tables affected by the Explicit Roles plugin.

**Tables affected by the Explicit Roles plugin**

| Table | Changes |
|---|---|
| Access Control<br><br>[sys_security_acl] | For all existing and newly created ACLs without a role requirement, the snc_internal role is assigned. |
| Catalog item<br><br>[sc_cat_item] | For all records where the **Roles** field is empty, the snc_internal role is added. If the glide.sc.use_user_criteria property is set to false, newly created catalog items are automatically assigned the snc_internal role. If the property is set to true, the SNC External user criteria is added to all newly created catalog items, excluding external users from viewing the record. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tables affected by the Explicit Roles plugin (continued)**

| Table | Changes |
|---|---|
| Page<br><br>[content_page] | For sites that have a login page, where the **Read roles** field is empty, the snc_internal role is added. For sites that have no login page or that have automatically created content pages, the public role is added. |
| Navigation Menu [sys_app_application] | For all records where the **Roles** field is empty, the snc_internal role is added. Newly created navigation menus with an empty **Roles** field are also automatically assigned the snc_internal role. |
| Overview Help Panel [sys_ui_overview_help_panel] | For all records where the **Roles** field is empty, the snc_internal role is added. Newly created overview panels with an empty **Roles** field are also assigned the snc_internal role. |
| Portal Page [sys_portal_page] | For all records where the **Read** roles field is empty, the snc_internal role is added. Newly created portal pages with an empty **Read roles** field are also automatically assigned the snc_internal role. |
| Processor [sys_processor] | For all records where the **Roles** field is empty, the snc_internal role is added. Newly created processors with an empty **Roles** field are also automatically assigned the snc_internal role. |
| Report [sys_report] | For all records where the **Roles** field is empty, snc_internal is added. Newly created reports that have an empty **Roles** field when sharing are also automatically assigned the snc_internal role. |

## Vendor Risk Overview reports — Legacy view

The Vendor Risk Overview page is replaced by the third-party risk reports on the Vendor Management Workspace.

## Viewing the reports

To open the Vendor Risk Overview, navigate to **All** > **Third-party Risk Management** > **Overview**. The page displays reports that provide insights into your third-party risk management program. The

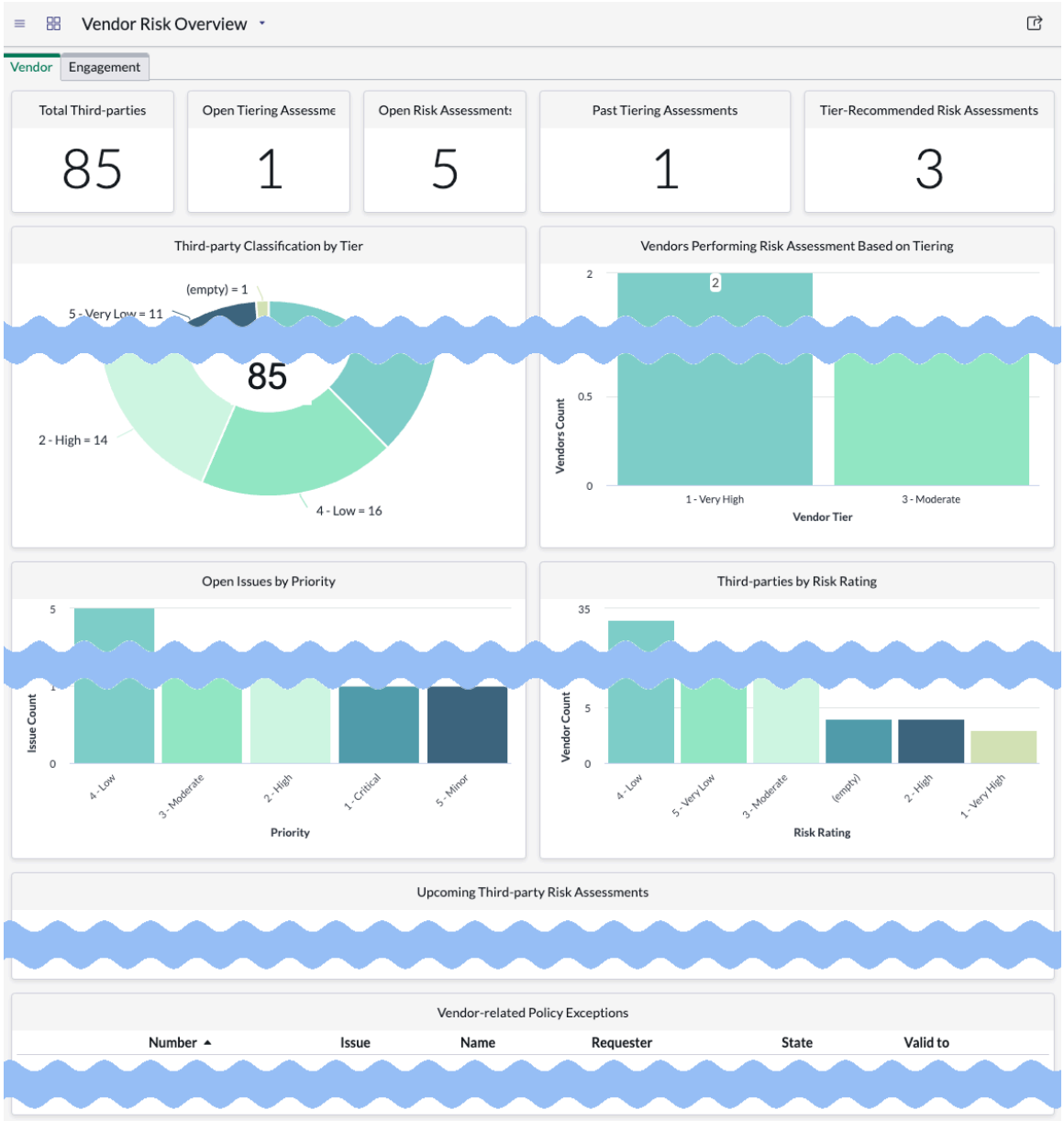
## The more complete IRQ process replaces tiering

In the TPRM application, the IRQ is an internal questionnaire that improves the original tiering assessment process. IRQs enhance internal risk assessments with increased flexibility, control, and scalability.

To enable a seamless transition to TPRM, you have the option to duplicate existing tiering assessments and designate them as IRQ internal assessments. Risk tiering is supported as an unchanging legacy process.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Vendor Risk Overview — Vendor tab




### Reports on the Vendor tab

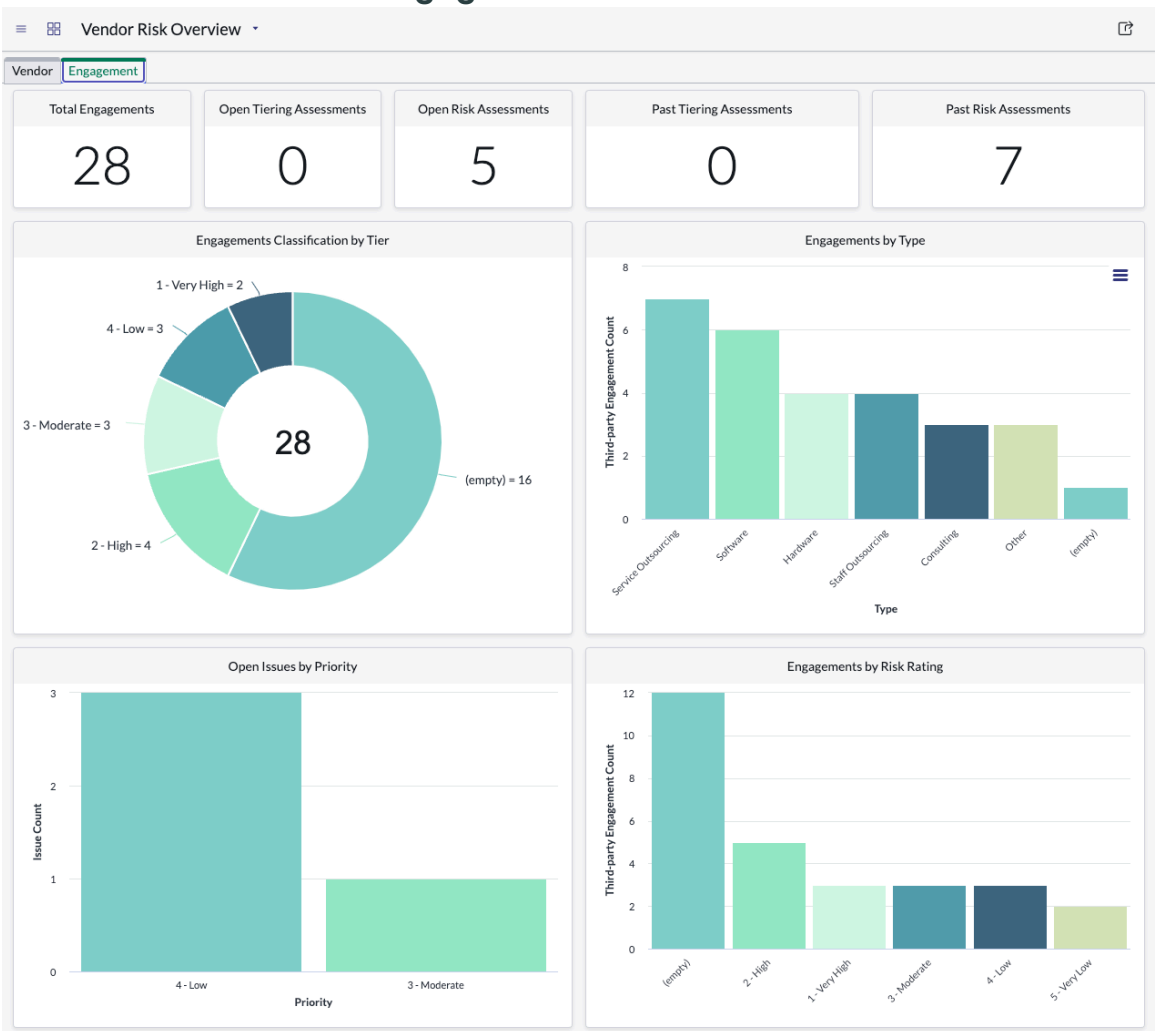
| Report | Description |
|---|---|
| Total Vendors | Total number of third parties. |
| Open Tiering Assessments | Number of third parties with active tiering assessments open. |
| Open Risk Assessments | Number of third parties with active risk assessments open. |
| Past Tiering Assessments | Number of third parties that have not completed the tiering assessment within the assessment time frame. |
| Tier-Recommended Risk Assessments | Number of third parties performing risk assessments based on tiering. |
| Vendor Classification by Tier | Donut report showing the number of third parties assigned to each risk tier. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Reports on the Vendor tab (continued)

| Report | Description |
|---|---|
| Vendors Performing Risk Assessment Based on Tiering | Number of third parties with active tiering-based risk assessments sorted by third-party risk. |
| Open Issues by Priority | All third-party risk open issues sorted by priority. |
| Vendors by Risk Rating | Number of third parties sorted by risk rating. |
| Upcoming Vendor Risk Assessments | Number of third-party risk assessments scheduled. |
| Vendor-related Policy Exceptions | All policy exceptions generated from third-party risk issues. |

## Vendor Risk Overview — Engagement tab




### Reports on the Engagement tab

| Report | Description |
|---|---|
| Total Engagements | Total number of engagements. |
| Open Tiering Assessments | Number of engagements with active tiering assessments open. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Reports on the Engagement tab (continued)**

| Report | Description |
|---|---|
| Open Risk Assessments | Number of engagements with active risk assessments open. |
| Past Tiering Assessments | Number of engagements that have not completed the tiering assessment within the assessment time frame. |
| Past Risk Assessments | Number of engagements with active tiering-based risk assessments. |
| Engagements Classification by Tier | Donut report showing the number of engagements assigned to each tier. |
| Engagements by Type | Number of engagements of each type. |
| Open Issues by Priority | All engagement open issues sorted by priority. |
| Engagements by Risk Rating | Number of engagements sorted by risk rating. |

# Common GRC features

Each of the four main Governance, Risk, and Compliance applications have unique features and capabilities. Additionally, there are many features that are common to all GRC applications.

For example, you can run GRC applications using the ServiceNow® mobile application. Content packs and integrations are available from multiple GRC applications. Information, such as domain separation support levels, are also included here.

## Mobile experience for Governance, Risk, and Compliance

Manage your work, task assignments, requests, approvals, and other follow-up actions for GRC applications directly from your mobile device. Receive timely notifications for current alerts, as well as risk and compliance status for your critical assets, vendors, and impacted essential business services.

Starting with New York, the following applications provide mobile access:

- Mobile experience for GRC Policy and Compliance
- Mobile experience for GRC Risk Management

## GRC application nomenclature updates and industry terminology

The following terms are used within GRC applications and/or within the GRC industry.

### GRC nomenclature updates

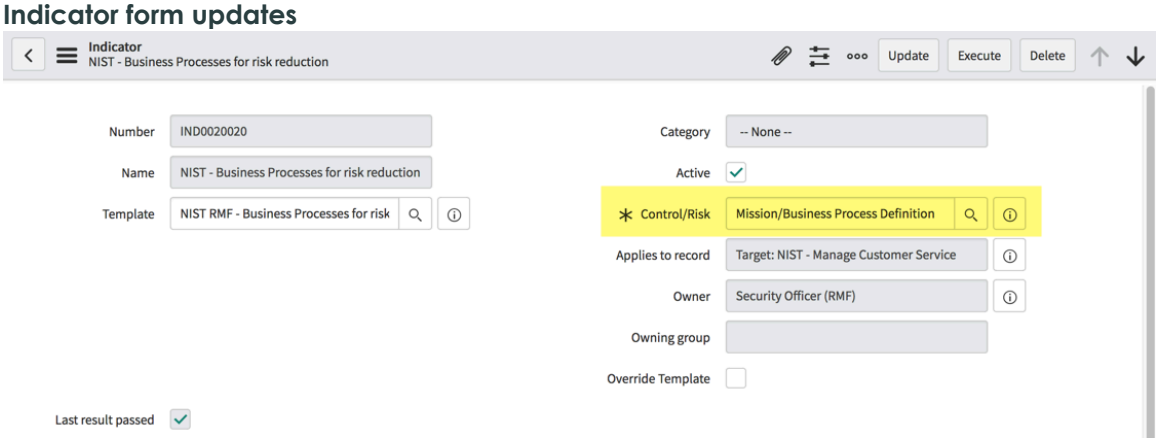
Starting with previous release, many terms within all the GRC core applications were updated.

**Note:** These term updates apply to all navigation labels, buttons, info messages, report titles, related links, tabs, and other UI elements.

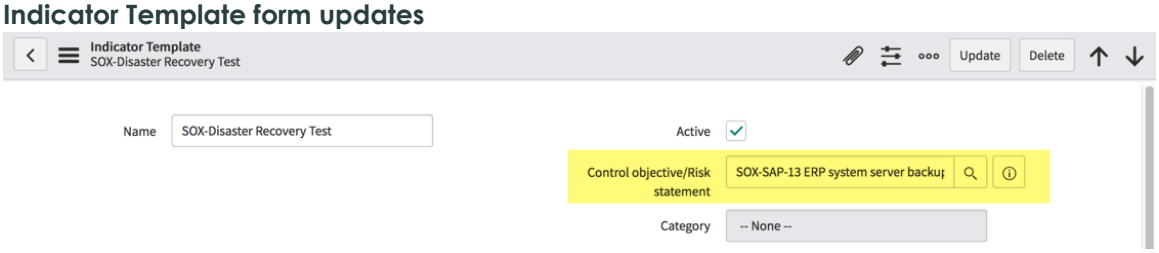
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| GRC module | Previous | Current |
|---|---|---|
| **Scoping** | **Profile** | **Entity** |
| | **Profile Types** | **Entity Types** |
| | **Profile Classes** | **Entity Classes** |
| | **My Profiles** | **My Entities** |
| | **All Profiles** | **All Entities** |
| **Administration** | **Profile Tiers** | **Entity Tiers** |
| | **Profile Class Rules** | **Entity Class Rules** |
| **Indicators** | **Indicators** > **Item** field | **Control/Risk** field |
| | | **Category** field indicates whether it is a compliance or risk indicator |
| | **Indicator Template** > **Content** field | **Control Objective/Risk Statement** |
| **Issues** | **Details** > **Content** field | **Control Objective/Risk Statement** |
| | **Details** > **Item** field | **Control/Risk** |
| **Policy and Compliance** | **Policy Statement** | **Control Objective** |
| **Risk** | **All Risks** > **Statement** > **field** | **My Risks** > **Risk Statement** field |
| | **My Risks** > **Statement** field | **My Risks** > **Risk Statement** field |

## Indicator form updates

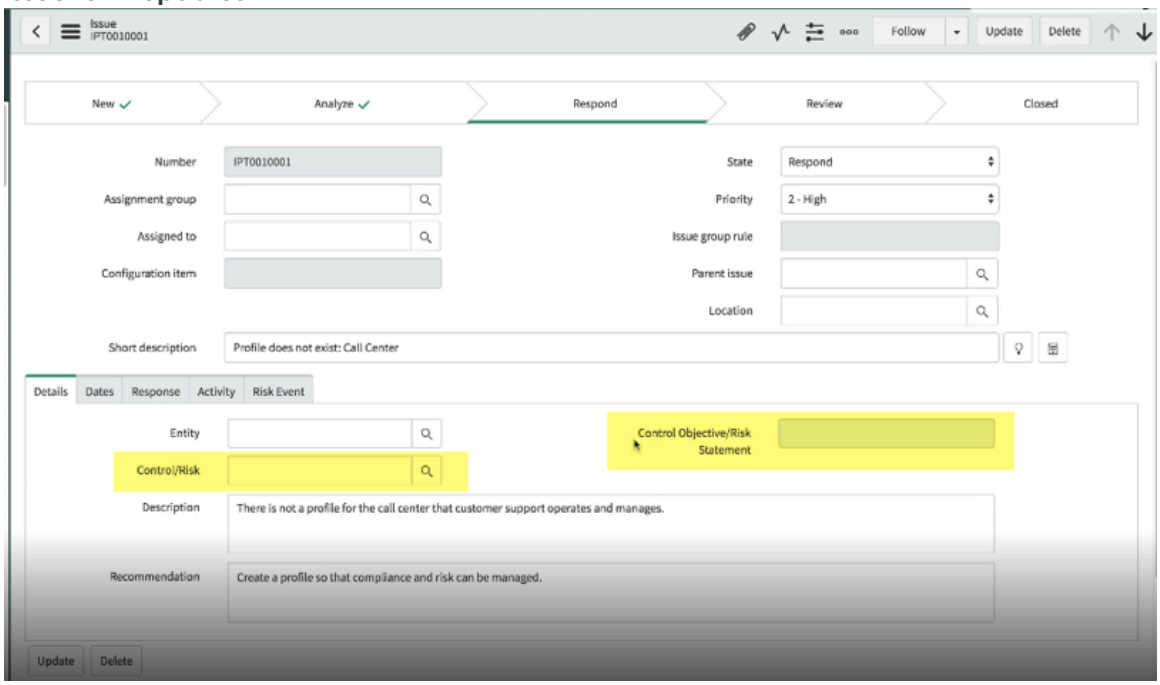



## Indicator Template form updates

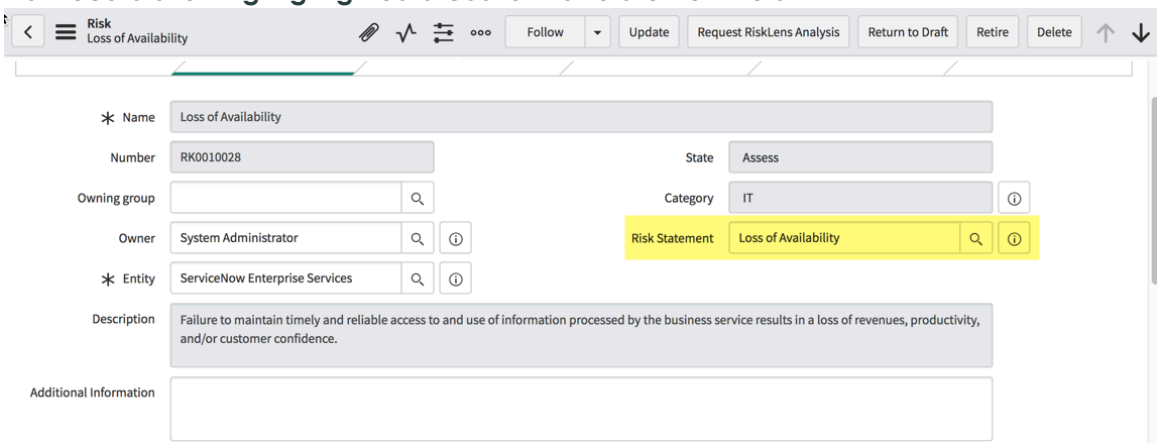



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Issue form updates




### Risk record showing highlighted areas for Risk Statement field




## Industry references

- ENISA Glossary
- ISACA Glossary
- ISO Risk Glossary
- OCEG Glossary
- PCI Compliance Guide

### Industry acronyms

| Term | Definition |
|---|---|
| Basel III | An international standard for banking that regulators can use when making regulations on how much capital banks must have to offset potential risk. The more risk a bank has, the more capital it should have in place to ensure that it stays solvent. The regulation was |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Industry acronyms (continued)

| Term | Definition |
|---|---|
| | the third such standard issued by the Basel Committee on Banking Supervision, and hence the name Basel III. |
| CISA | Cybersecurity Information Sharing Act |
| CISM | Certified Information Security Manager |
| COBIT | Control Objectives for Information and Related Technologies (COBIT) provides an IT governance framework to manage risk and compliance issues based on best practices. Published by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA). |
| COSO | The Committee of Sponsoring Organizations (COSO) was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting. COSO is an independent private sector initiative that studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies, the SEC, and other regulators and educational institutions. |
| EDPA | European Data Privacy Act |
| ENISA | European Network & Information Security Agency |
| EUP | Energy use in products (EUP) is an EU directive that requires companies to design products to use less energy. |
| European Directive on Data Protection | One of the first and most important pieces of data privacy legislation that specifically addresses internet privacy. |
| FCA | Financial Conduct Authority |
| GDPR | General Data Protection Regulation (GDPR) is a regulation, effective May 25, 2018, replacing the Data Protection Directive 95/46/ec to strengthen and harmonize the data protection rights of European Union citizens. |
| GRI | Global Reporting Initiative (GRI) is an international group that created the G3 framework for sustainability reporting. |
| ITGI | IT Governance Institute |
| PII | Personal Identifying Information / Personally Identifiable Information (PII) is the information that permits the identity of an individual to be directly or indirectly inferred. |
| PCI DSS | Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. |
| SOLVENCY II | SOLVENCY II |
| SOX | The Sarbanes-Oxley Act (SOX) established the Public Company Accounting Oversight Board and added requirements for publicly traded companies, their officers, boards, and auditors. It increased penalties for corporate financial fraud. This U.S. Legislation was enacted in response to the high profile Enron and WorldCom financial scandals. Its goal is to protect shareholders and the general public from accounting errors and fraudulent practices in |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Industry acronyms (continued)

| Term | Definition |
|---|---|
| | the enterprise. SOX applies to companies that trade publicly in the U.S. |

### Industry terms

| Term | Definition |
|---|---|
| ALE | Annualized loss expectancy (ALE) = Single Loss Expectancy (SLE) x Annualized Rate of Occurrence (ARO). Used in Quantitative risk scoring. |
| ARO | Annualized rate of occurrence. |
| Acceptance | A specific risk can be accepted by the management, stopping further investments into deeper controls or higher levels of mitigation, if it is within the level of Tolerance or if further mitigation and control would actually cost much more that the estimated Impact (or significance) of the risk. |
| Assertion | Any formal declaration or set of declarations about the subject matter made by management. |
| Assessment | A broad review of the different aspects of a company or function that includes elements not covered by a structured assurance initiative. |
| Attestation | Process of validating that something is true. For instance, a control effectiveness or compliance can be attested through a questionnaire, electronically signed by its fulfiller. |
| Audit | Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met. In ServiceNow®, an organization identifies all the controls that they want to test at one time and assigns responsibility of the overall audit to a single person. A single task manages the testing of all controls. |
| Audit activities | One of the tasks within an audit that is assigned to an individual for execution of the audit. |
| Audit committee | A committee, often including members of the board of directors, responsible for overseeing financial reporting and internal controls. |
| Audit documentation (working papers) | Records kept by the auditor of procedures applied, tests performed, information obtained, and pertinent conclusions reached in the engagement. The documentation provides the principal support for the auditor's report. |
| Audit evidence | Facts gathered during the audit procedures that provide a reasonable basis for forming an opinion regarding the financial statements under audit. |
| Audit objective | When obtaining evidence in support of financial statement assertions, the auditor develops specific audit objectives in light of those assertions. For example, an objective related to the |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Industry terms (continued)

| Term | Definition |
|---|---|
| | completeness assertion for inventory balances is that inventory quantities include all products, materials, and supplies on hand. |
| Audit observations | Used by internal auditors for identifying control gaps or identifying new risks. |
| Automated controls | Internal controls executed automatically by computer systems. Manual controls are executed by a person charged with that task and are typically performed on a subset of transactions and data. Automated controls can be executed on every relevant transaction or data element, ensuring greater accuracy with less effort. |
| Authority documents | The regulations, certifications, frameworks, standards, and best practices that an organization chooses or are required for compliance with regulations. Authority Documents are related to controls, risks, and policies. |
| Business risk | Risks that could adversely affect an entity's ability to achieve its objectives and execute its strategies. |
| Calculated score | Calculated score is derived from the inherent score and residual score as an overall outcome. Refers to actual exposure of risk based on the quality of implemented control system. |
| Chain of custody | A legal principle regarding the validity and integrity of evidence. It requires accountability for anything used as evidence in a legal proceeding. This ensures that it can be accounted for from the time it was collected until the time it is presented in a court of law. |
| Chief Compliance Officer (CCO) | A corporate official in charge of overseeing and managing compliance issues within an organization. This person ensures that a company is complying with regulatory requirements, and that the company is complying with internal policies and procedures. |
| Chief Operating Officer (COO) | Also called a Chief Operations Officer, an executive in charge of the company's day#to#day operations. |
| Chief Risk Officer (CRO) | Also called a Chief Risk Management Officer, an executive in charge of enterprise risk management and the compliance efforts of a company. |
| Citations | Records with the specific requirements cited by an authority document. The citation record relates authority documents to its applicable control. |
| Compliance | The act of adhering to and demonstrating adherence with laws, regulations, or policies. Compliance relates to regulations in many areas including finance, the environment, global trade, worker safety, and privacy. |
| Confidentiality | Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information. |
| Containment control | Control designed to limit the impact (or significance) of a risk, if it would occur. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Industry terms (continued)

| Term | Definition |
|---|---|
| Control | The actual control activities that are performed by an organization. Control records include basic required information about the control (owner, activity, frequency, and so forth.). Controls can be related to authoritative source contents, policies, and risks.<br><br>Any action taken by management, the board, and other parties to manage risk. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals are achieved. Control records include basic required information about the control (owner, activity, frequency, and so forth.). Controls can be related to authoritative source contents, policies, and risks. |
| Control framework | A set of fundamental controls which perform and preserve the cross mapping of controls to prevent financial loss, information loss, or more generally to prevent risks within an enterprise. |
| Control instance | The actual run of a Control Test Definition, periodically or on demand, showing the result data sample, the attestation, or the manual result of the test activities. |
| Control test definitions | Control test definitions specify how and when controls are tested, including testing steps, expected results, the group or individual responsible for the testing, and the test schedule. Control test instances are automatically generated from the test schedule. Remediations are automatically created when control tests fail or when audit observations are noted. |
| Corrective controls | Internal controls that come into play once a problem is discovered. An example would be removing access from users who have excessive privileges or executing a backup and recovery plan after a physical disaster has occurred. |
| Corporate Performance Management | Corporate Performance Management (CPM) is a combination of strategy management, planning, reporting and consolidation, and revenue, cost, and profitability modeling that enables companies to measure their performance and improve it. |
| Detect | Ongoing progress toward objectives as well as actual and potential undesirable conditions and events using management actions and controls. |
| Detective control | A control designed to discover an unintended event or result. It may also detect if and when a specific risk occurs. |
| Effect | A measure of the likelihood, timing, and impact of an event on something. |
| Effective internal control | Reasonable assurance that operational objectives are achieved, that published financial statements are reliably prepared, and that the entity complies with applicable laws and regulations. |
| Engagement | An audit project that may include audit tasks that accomplish a set of objectives or goals. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Industry terms (continued)

| Term | Definition |
|---|---|
| Event | An observable action, occurrence, or a change in condition. An event includes change in knowledge about a condition, even if the condition did not change. |
| Entity | Fundamental concept of GRC, entities are used to model any enterprise element for which controls and risks can be associated. For example: business units, servers, laptops. |
| Entity type | Used to refer to multiple similar entities. For example: Asia/Pacific business unit, Linux servers, MacBook Pro. |
| Evaluate | To measure something against criteria. |
| Evidence (evidential matter) | Includes written and electronic information (such as checks, records of electronic fund transfers, invoices, contracts, and other information) that permits the auditor to reach conclusions through reasoning. |
| Fraud | Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services and to avoid payment or loss of services or to secure personal or business advantage. |
| General controls | Policies and procedures to assure proper operation of computer systems, including controls over network operations, software acquisition and maintenance, and access security. |
| Governance, Risk, and Compliance (GRC) | Governance, risk management, and compliance with regulations have traditionally been separate corporate functions. GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives while addressing uncertainty and acting with integrity. It encompasses the governance, assurance and management performance, risk, and compliance.<br><br>GRC is the business of how an organization operates through the management of risk while remaining compliant with external and internal standards to optimize performance. GRC embraces how processes, controls, security, and culture integrate to ensure that the organization has integrity. |
| Impact | Used to evaluate the severity of a risk, together with the Likelihood. It evaluates the level of consequence a specific risk would have on an organization if/when it would occur. |
| Indicator | A metric used to collect data to monitor controls and risks, and collect audit evidence. |
| Inherent likelihood | The likelihood of the identified risk occurring before any response strategy is implemented. |
| Inherent risk | The level of risk exposure, in terms of Likelihood and Impact (or significance), assuming no related internal controls and no mitigation actions are yet in place. |
| Inherent score | The score of the risk before any response strategy is implemented. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Industry terms (continued)

| Term | Definition |
|---|---|
| Inherent significance | How significant the risk is before any response strategy is implemented. |
| Integrity | The property whereby information, an information system, or a component of a system has not been modified or destroyed in an unauthorized manner.<br><br>A state in which information has remained unaltered from the point it's produced by a source, during transmission, storage, and eventual receipt by the destination. |
| Internal audit | A department, division, team of consultants, or other practitioners that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes. |
| Internal auditors | Employees of the client responsible for providing analyses, evaluations, assurances, recommendations, and other information to the entity's management and board. An important responsibility of internal auditors is to monitor performance of controls. |
| Internal controls | The policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected. |
| Issue | A GRC task that allows end users to document Control and Risk issues and track the response to remediate or accept the issue. |
| IT Governance | The leadership, organizational structures, and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives. It is the responsibility of executives and the board of directors. |
| IT GRC | Encompasses the software and hardware and related policies and procedures used to support compliance and risk management efforts from an IT perspective based on established best practices. |
| Likelihood | The probability that something happened. |
| Management | The act of internally directing, controlling, and evaluating an entity, process, or resource. |
| Manual controls | Controls performed manually, not by computer. |
| Material (materiality) | A risk is material when it is possible to calculate its financial impact. |
| Mitigation | Reducing the risk associated with a particular violation of a rule. Before a risk occurs, appropriate mitigation actions are put in place to resolve possible related control failures and/or to reduce the risk exposure. |
| Objective | Something that an entity intends to attain or accomplish. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Industry terms (continued)

| Term | Definition |
|---|---|
| Operational audit | An audit designed to evaluate the various internal controls, economy, and efficiency of a function or department. |
| Operational controls | Controls relating to the daily operation of a company or enterprise to ensure that all objectives are achieved. |
| Operational risks | Risks relating to the people, processes, and systems required to achieve an organization's mission and objectives. |
| Objectivity | The ability to evaluate client records with no preconceived notions or prejudices. |
| Obligations | Assertions about obligations deal with whether liabilities are obligations of the entity at a given date. For example, management asserts that amounts capitalized for leases in the balance sheet represent the cost of the entity's rights to leased property and that the corresponding lease liability represents an obligation of the entity. |
| Owner | The owner of a risk, a control, or a mitigation/remediation task accepts its accountability. They may delegate some tasks related to the ownership, but they stay accountable to the organization. |
| Peer review | A practice monitoring program in which the audit documentation of one CPA firm periodically reviewed by independent partners of other firms to determine that it conforms to the standards of the profession. |
| Plan | Audit planning is developing an overall strategy for conduct and scope of the audit. The nature, extent, and timing of planning vary with size and complexity of the entity, experience with the entity, and knowledge of the business. In planning the audit, the auditor considers the entity's business and its industry, its accounting policies and procedures, methods used to process accounting information, the planned assessed level of control risk, and the auditor's preliminary judgment about audit materiality. |
| Policy | A document that records a high#level principle or course of action that has been decided on. The intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives, and strategic plans established by the enterprise's management teams. In addition to policy content, policies describe the consequences of failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy is checked and measured.<br><br>In ServiceNow®, approved policies are published in the Knowledge Base. Policies are related to authority documents and control records. Policy statements define specific details that a process follows within a policy. |
| Preventative control | A control designed to avoid an unintended event. |
| Procedure | An action, such as a step performed as part of an audit program or as part of the client's internal controls. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Industry terms (continued)

| Term | Definition |
|---|---|
| | Provides the "how to" of policies and guides their implementation. Procedures are audience-specific and provide exact instructions that ensures compliance with a given policy. ServiceNow® treats policies and procedures in the same way; therefore, the terms may be used interchangeably. This may differ from frameworks, such as COBIT 5.1, which defines policies and procedures as two separate items. |
| Professional skepticism | Approaching an audit with a questioning mind-set. |
| Qualitative Impact | Includes Impact (refers to significance of a risk) and Likelihood (refers to probability of a risk occurring) ratings. Score is calculated by multiplying Impact by Likelihood. An impact often expressed using an ordinal scale or nominal scale. |
| Quantitative Impact | A positive/negative effect on financial assets, tangible assets, intangible assets, business continuity, and health & safety. Calculated by Single Loss Expectancy (SLE) x Annualized Rate of Occurrence (ARO) = Annualized loss expectancy (ALE). A quantitative impact is expressed numerically. |
| Questionnaire | An internal control questionnaire is a list of questions about the internal control system to be answered (with answers such as yes, no, or not applicable) during audit fieldwork. The questionnaire is part of the documentation of the auditor's understanding of the client's internal controls. |
| Random sample (random-number sampling) | Identical probability of each population item being selected for a sample. Also, the use of random numbers to select a random sample from a population. |
| Reasonable assurance (an internal control) | An internal control, no matter how well designed and operated, cannot guarantee that an entity's objectives are met because of inherent limitations in all internal control systems. |
| Remediation | After a failure is identified and assessed, appropriate remediation can take place to mitigate or eliminate the issue Residual likelihood: The likelihood of the identified risk occurring after any response strategy is implemented. |
| Requirement | Something that an entity must address as a result of making a promise. |
| Residual likelihood | The likelihood of the identified risk occurring after any response strategy is implemented. |
| Residual risk | Level of the risk exposure, in terms of likelihood and impact (or significance), after related internal controls and mitigation actions are in place and effective. |
| Residual score | The score of the risk after any response strategy is implemented. |
| Residual significance | How significant the risk is after any response strategy is implemented. |
| Risk | A risk is any threat or vulnerability that could adversely affect an organization's business objectives. All risks are contained in one risk |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Industry terms (continued)

| Term | Definition |
|---|---|
| | repository. Risks can be related to any item, policy, control, and remediation task. Risks requiring immediate or ongoing attention can be mitigated, prevented, or controlled using the defined controls and related control tests. A risk statement is a defined consequence that can occur if a threat exploits a vulnerability.<br><br>Risk is measured in terms of Impact (or Significance) and Likelihood. Types of risks include operational risks (fraud, for example), risks of noncompliance (not filing the proper documents to comply with legislation), and strategic risks (such as an incident that affects a brand's reputation). The business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise. |
| Risk analysis | The systematic examination of available information to determine how often specified events may occur and the magnitude of their consequences. |
| Risk appetite | The level of risk that an organization is willing to accept in pursuit of its objectives. |
| Risk assessment | The appraisal of the risks facing an entity, asset, system or network, organizational operations, individuals, geographic area, other organizations, or society, and includes determining the extent to which adverse circumstances or events could result in harmful consequences. |
| Risk criteria | Are quantitative or qualitative values against which level of risk is evaluated. |
| Risk management | The objective of risk management is to reduce uncertainty. It's the act of managing processes and resources to address risk while pursuing the organization's objectives. The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken. |
| Risk management framework | A formalized process for managing risk on an explicit basis. The framework consists of a risk assessment, response, and accountability for the risk and mitigation activities around it. |
| Risk mitigation | The processes built into the controls environment, such as policies, frameworks, and accountabilities, that reduce a risk. |
| Risk register | A repository of the key attributes of potential and known IT risk issues. Attributes may include name, description, owner, expected/ actual frequency, inherent/residual level, potential/actual business impact, and mitigation/remediation plans. |
| Risk response | The decision to accept a risk, decline a risk, treat or mitigate a risk, or share a risk with another party. |
| Risk statement | General statements about potential risks or threats that could occur somewhere in an organization. |
| Risk tolerance | The level of risk that the organization is unwilling to exceed to achieve objectives. The representation of the risk appetite in terms |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Industry terms (continued)

| Term | Definition |
|---|---|
| | of threshold, generally financial, given to various management levels in the organization for specific risk categories. |
| Sample size | The number of population items selected when a sample is drawn from a population. |
| Sampling | Selecting a small but pertinent and representative number of records to represent the entire population of records. |
| Sampling risk | The possibility that conclusions drawn from the sample may not represent correct conclusions for the entire population. |
| Segregation of duties (SoD) | Assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets. Segregation of duties reduces the opportunities for one person to both perpetrate and conceal errors or fraud. |
| Significance | Used to evaluate the severity of a risk, together with the Likelihood. It evaluates the level of consequence a specific risk would have on an organization if/when it would occur. |
| SLE | Single loss expectancy (SLE) = Single Loss Expectancy = Asset Value x Exposure Factor. |
| Stakeholder | A person, group, or organization that has direct or indirect stake in an organization because it can affect or be affected by the organization's actions, objectives, and policies. |
| Standard | A professional pronouncement promulgated by the Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities, and for evaluating internal audit performance. |
| Strategic risks | Relating to strategic objectives such as political factors, customer priorities, brand, or reputation. |
| Target | A measurable value that an entity strives to achieve. |
| Test | A sample from a population to estimate characteristics of the population. |
| Test plan | A specific audit test of the design and operating effectiveness of a single control. |
| Threat | An event that has, on balance, an undesirable effect on achieving objectives. |
| Tolerance | The acceptable level of departure from a target. |
| Unified Compliance Framework (UCF) | Network Frontiers Unified Compliance Framework (UCF) contains authority documents that can be imported into the ServiceNow® instance. For more information, see Unified Compliance Framework. |
| Uncertainty | The state of being unable to completely predict, determine, or define something. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# GRC content packs

Content packs may include pre-defined scopes, specific policies, controls, risks, audit, test plans, dashboards, and reports that provides customers an operational head-start when adopting various regulations and frameworks.

Use the following documentation for the installation, verification, and reporting features of the GRC content packs on the ServiceNow Store.

Unless otherwise noted, each content pack requires that you have the ServiceNow GRC products installed and activated on your instance.

## Sarbanes-Oxley (SOX) Content Pack

The Sarbanes-Oxley (SOX) Content Pack provides basic SOX content for an organization to commence and manage activities towards attaining operational SOX compliance using the ServiceNow® GRC application. A content pack may include pre-defined scope, specific policies, controls, risks, audit, test plans, dashboards, and reports providing users of ServiceNow® GRC a head-start in using the applications towards SOX compliance-related activities.

Users with the GRC Administrator roles of Compliance Admin (sn.compliance.admin), Risk Admin (sn.risk.admin), or Audit Admin (sn.audit.admin) in an organization are responsible for editing the content to suit the SOX requirements of the organization. The SOX Content Pack covers the three ServiceNow® GRC core applications, namely Policy and Compliance Management, Risk Management and Audit Management, and it establishes relationships across the various content elements in those applications.

### Install the SOX Content Pack

Install the SOX Content Pack for use with the core GRC applications.

**Before you begin**
Role required: sn_compliance.admin, sn_risk.admin, or sn_audit_admin, admin

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation.

| Setup task | Description |
|---|---|
| Verify that the ServiceNow plugins are activated. | Activate one of the following GRC plugins:<br>• GRC: Policy and Compliance Management (com.sn_compliance)<br>• GRC Risk Management (com.sn_risk)<br>• GRC: Audit Management (com.sn_audit)<br><br>To verify that this plugin is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Enter info re: Legal Notice.
2. If you have not installed the application, follow the instructions to install it.

   a. Log in to the instance you want to install the application on.

   b. Navigate to **System Applications** > **All Available Applications** > **All**.
   A list of apps available for installation is displayed.

   c. Locate the app, select it, and click **Install**.

   Your app is automatically installed onto your instance.

   When uninstalling the app, select the check box to retain the profile types profiles and indicators.

#### Verify the SOX Content Pack in Policy and Compliance Management

After importing the SOX Content Pack, verify and edit the profile types, profiles, policies, policy statements, controls, policies, indicator templates, and indicators, within the Policy and Compliance Management application.

### Before you begin

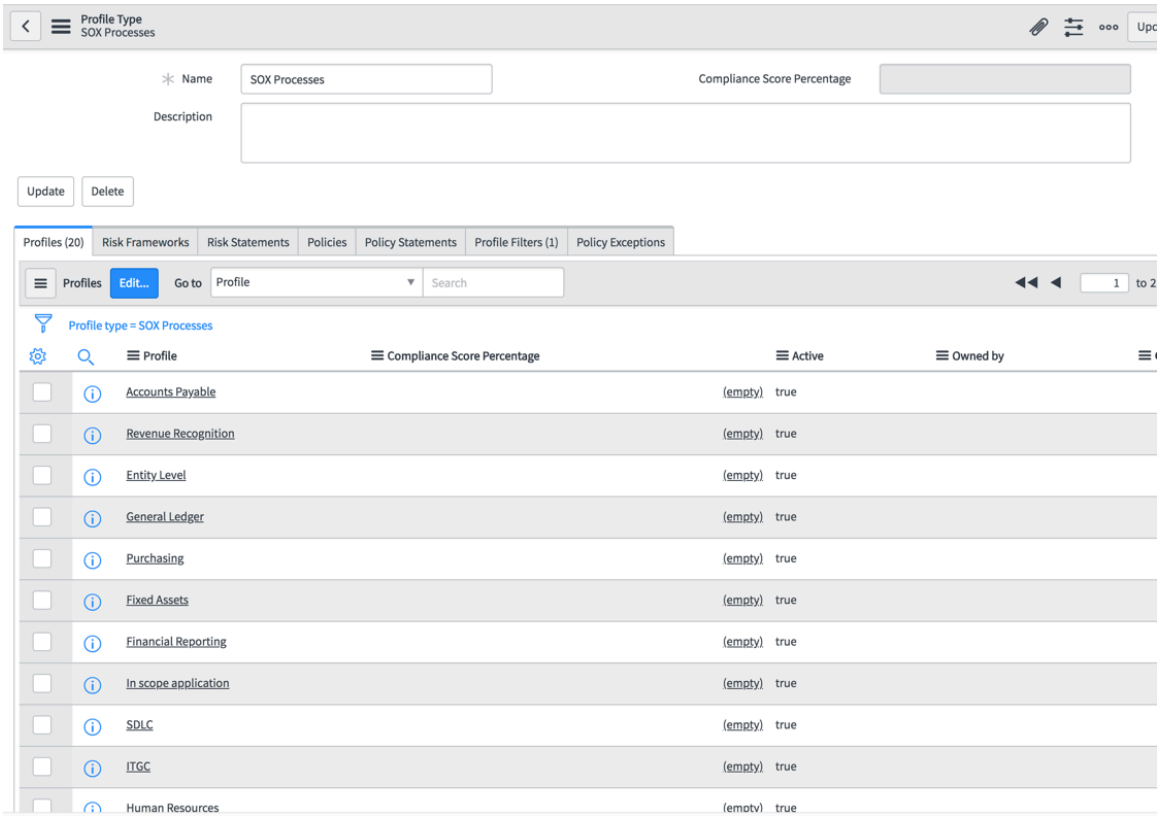
Role required: Compliance Admin (sn_compliance.admin)

### Procedure

1. Navigate to **All** > **Policy and Compliance** > **Scoping** > **Entity Types**.
   A **SOX Processes** entity type is added and is used to generate the SOX profiles:
   - Accounts Receivable
   - Accounts Payable
   - Commissions
   - Equity
   - Entity Level
   - Financial Reporting
   - Fixed Assets
   - General Ledger
   - Human Resources
   - In Scope Application
   - Inventory
   - ITGC
   - Payroll
   - Purchasing
   - Revenue Recognition
   - SAP
   - SDLC
   - Tax

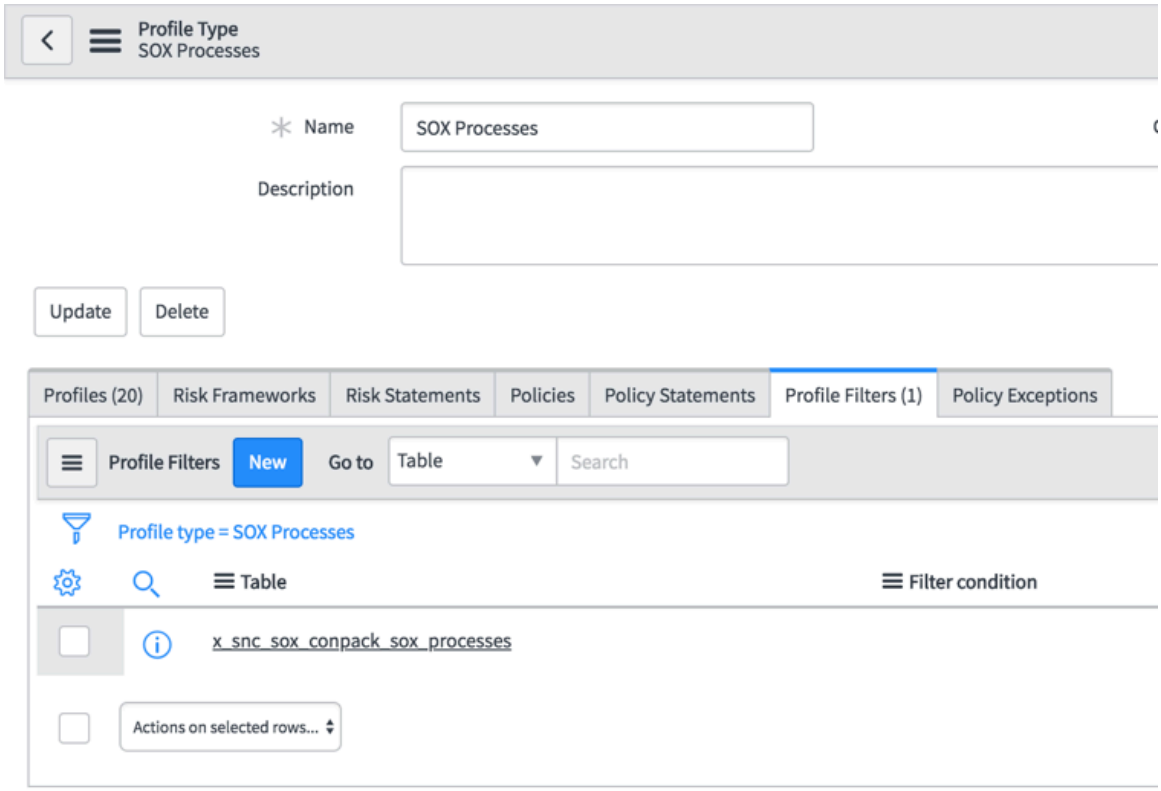
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Travel and Expense
- Treasury

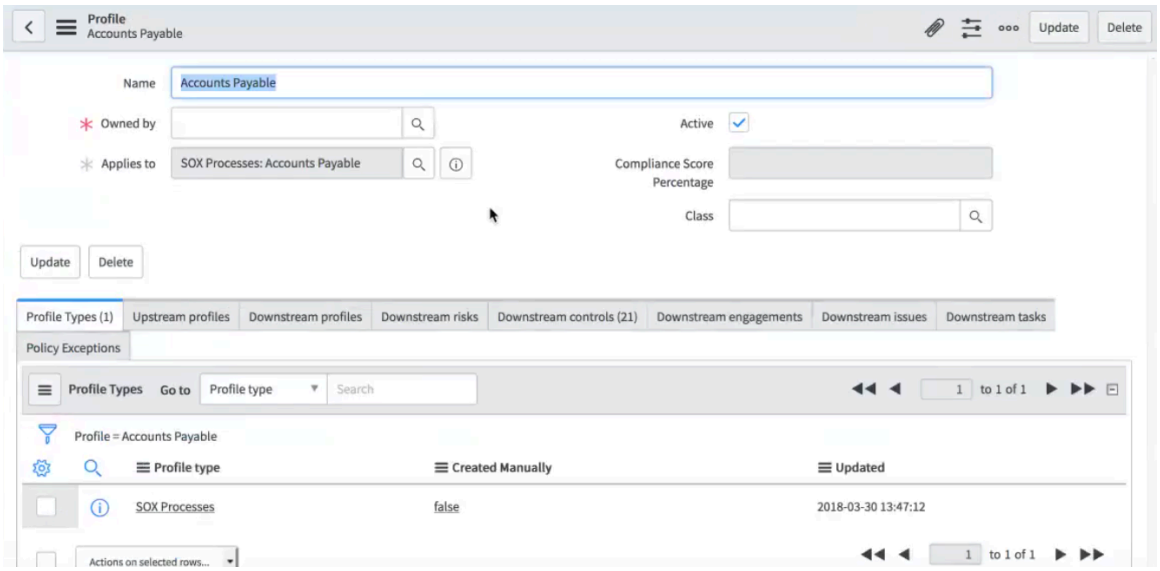



**2.** If using the Kingston SOX contact pack, under the Entity filters related list, a filter is added to query the SOX processes table for the generation of SOX entities.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**3.** Open an entity to see all the downstream controls.

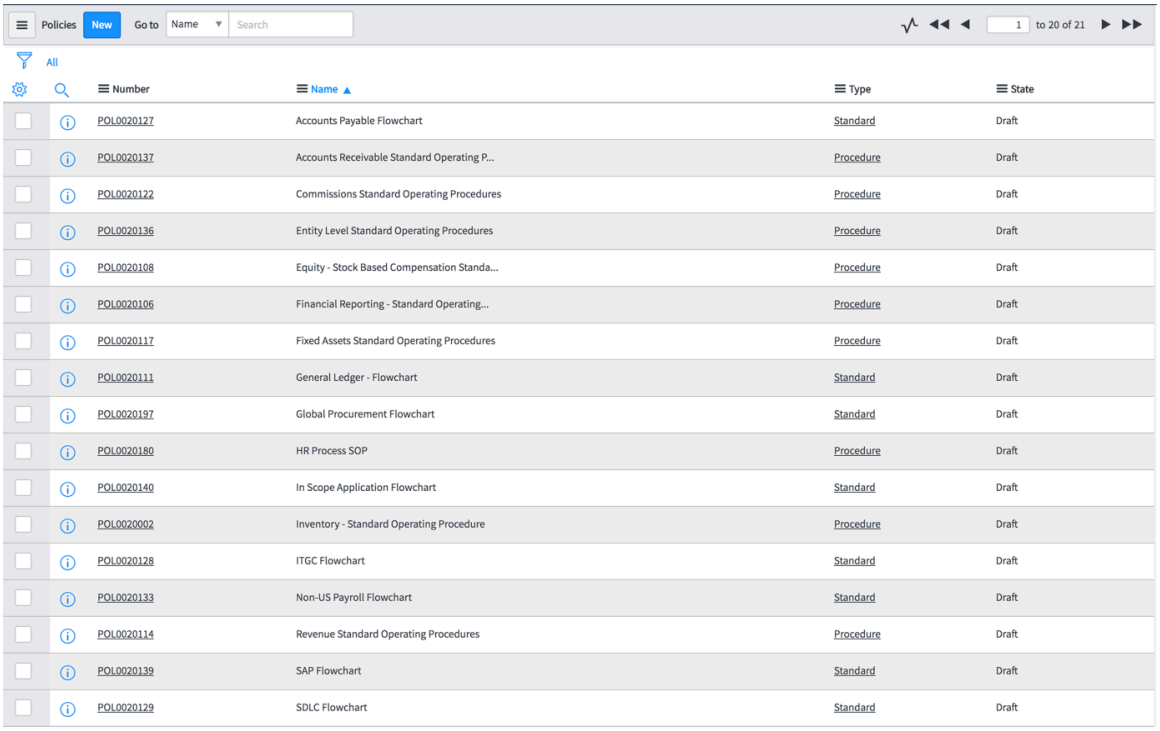



**4.** Navigate to **Policy and Compliance** > **Policies and Procedures** > **Policies**.
All SOX policies have been added in the Draft state:

- Accounts Payable Flowchart
- Accounts Receivable Standard Operating Procedures
- Commissions Standard Operating Procedures
- Entity Level Standard Operating Procedures
- Equity - Stock Based Compensation Standard Operating Procedures

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

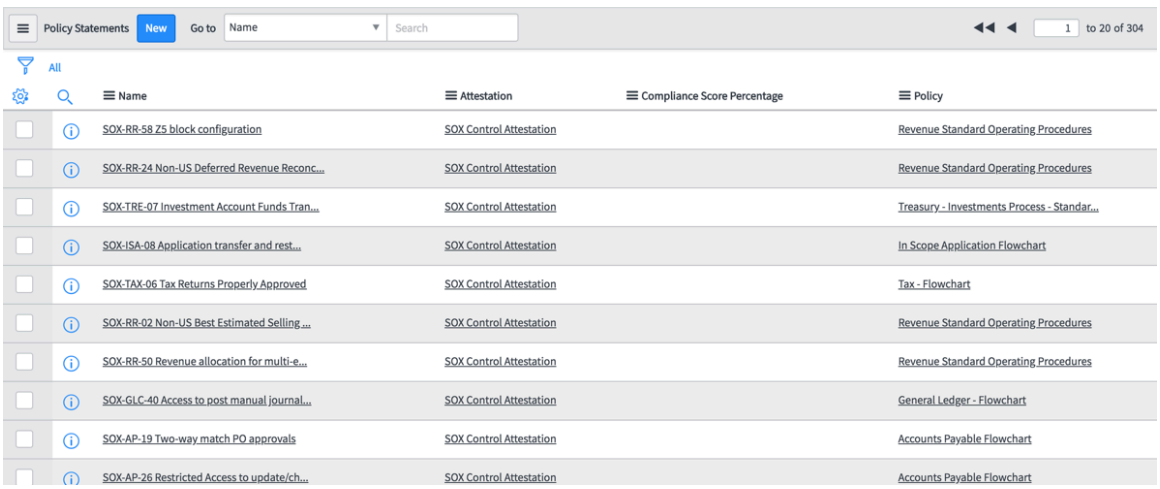
- Financial Reporting - Standard Operating Procedure
- Fixed Assets Standard Operating Procedures
- General Ledger - Flowchart




5. Open a SOX policy record.
   Notice that there is no text in the policy. Create your own policy and initiate the policy lifecycle.
6. Navigate to **Policy and Compliance** > **Policies and Procedures** > **Policy Statements**.
7. In the search bar, enter `SOX` in the **Name** field.

**Note:** The names of all SOX-related policy statements begin with **SOX**.

- All the SOX policy statements are created and assigned to SOX policies.
- The SOX Control Attestation is created and added to the policy statement.

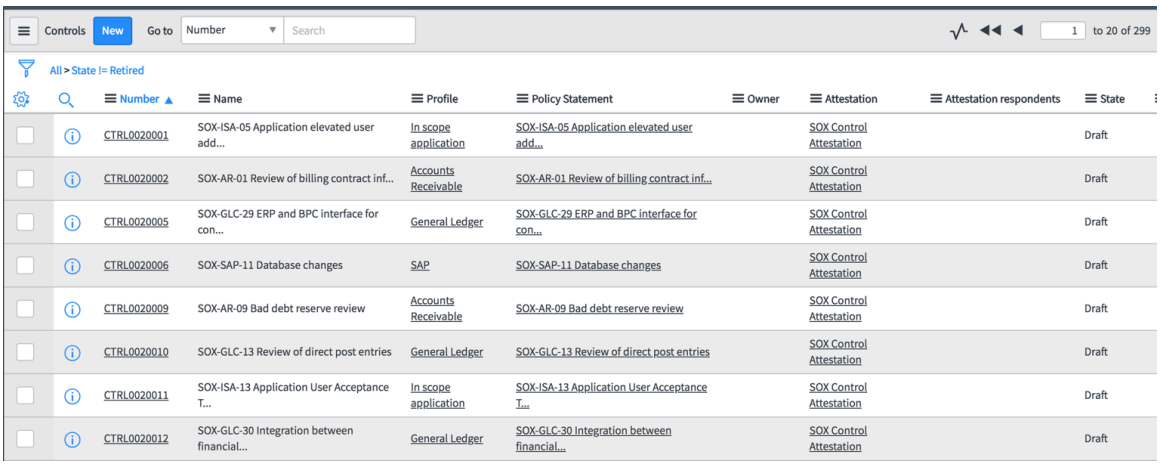



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Navigate to **Policy and Compliance** > **Controls**.
9. In the search bar, enter `SOX` in the **Name** field.

**Note:** The names of all SOX-related controls begin with **SOX**.

- All the SOX controls are created for each entity.
- The SOX Control Attestation is added to all controls with no attestation respondents.

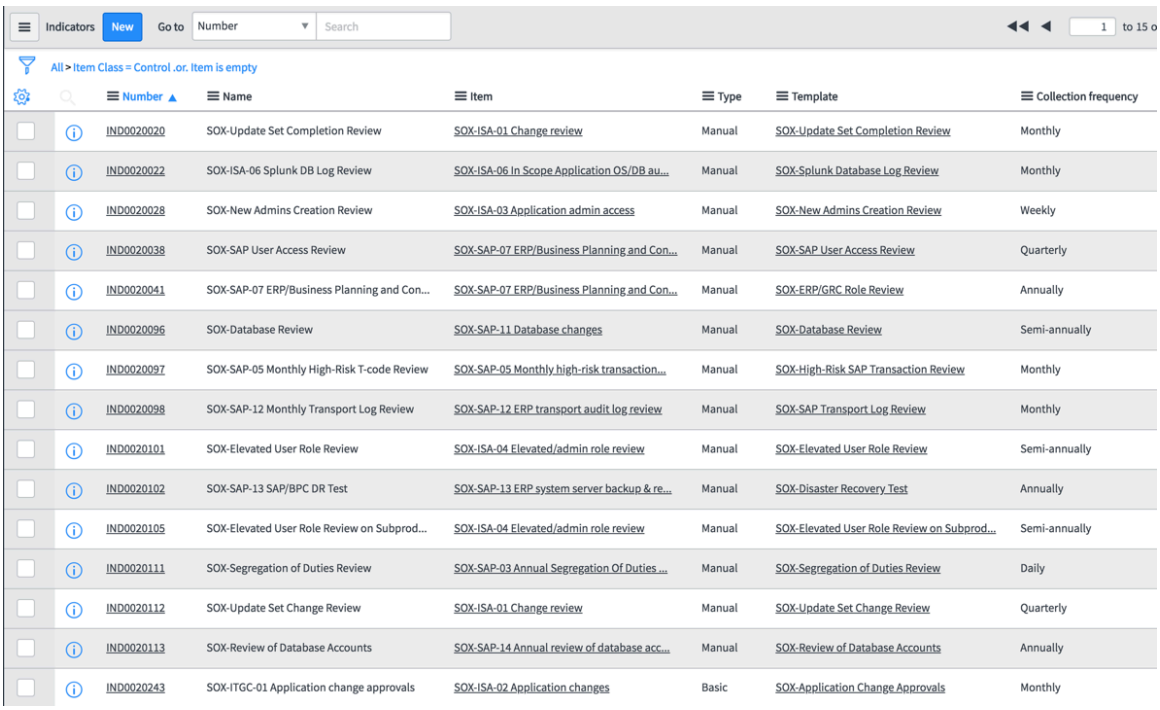


Controls | New | Go to | Number | Search | 1 to 20 of 299

All > State != Retired

| Number | Name | Profile | Policy Statement | Owner | Attestation | Attestation respondents | State |
|---|---|---|---|---|---|---|---|
| CTRL0020001 | SOX-ISA-05 Application elevated user add... | In scope application | SOX-ISA-05 Application elevated user add... | | SOX Control Attestation | | Draft |
| CTRL0020002 | SOX-AR-01 Review of billing contract inf... | Accounts Receivable | SOX-AR-01 Review of billing contract inf... | | SOX Control Attestation | | Draft |
| CTRL0020005 | SOX-GLC-29 ERP and BPC interface for con... | General Ledger | SOX-GLC-29 ERP and BPC interface for con... | | SOX Control Attestation | | Draft |
| CTRL0020006 | SOX-SAP-11 Database changes | SAP | SOX-SAP-11 Database changes | | SOX Control Attestation | | Draft |
| CTRL0020009 | SOX-AR-09 Bad debt reserve review | Accounts Receivable | SOX-AR-09 Bad debt reserve review | | SOX Control Attestation | | Draft |
| CTRL0020010 | SOX-GLC-13 Review of direct post entries | General Ledger | SOX-GLC-13 Review of direct post entries | | SOX Control Attestation | | Draft |
| CTRL0020011 | SOX-ISA-13 Application User Acceptance T... | In scope application | SOX-ISA-13 Application User Acceptance T... | | SOX Control Attestation | | Draft |
| CTRL0020012 | SOX-GLC-30 Integration between financial... | General Ledger | SOX-GLC-30 Integration between financial... | | SOX Control Attestation | | Draft |

10. Navigate to **Policy and Compliance** > **Indicators**.
SOX Control Indicators were added and indicator templates were assigned to them.



Indicators | New | Go to | Number | Search | 1 to 15 o

All > Item Class = Control .or. Item is empty

| Number | Name | Item | Type | Template | Collection frequency |
|---|---|---|---|---|---|
| IND0020020 | SOX-Update Set Completion Review | SOX-ISA-01 Change review | Manual | SOX-Update Set Completion Review | Monthly |
| IND0020022 | SOX-ISA-06 Splunk DB Log Review | SOX-ISA-06 In Scope Application OS/DB au... | Manual | SOX-Splunk Database Log Review | Monthly |
| IND0020028 | SOX-New Admins Creation Review | SOX-ISA-03 Application admin access | Manual | SOX-New Admins Creation Review | Weekly |
| IND0020038 | SOX-SAP User Access Review | SOX-SAP-07 ERP/Business Planning and Con... | Manual | SOX-SAP User Access Review | Quarterly |
| IND0020041 | SOX-SAP-07 ERP/Business Planning and Con... | SOX-SAP-07 ERP/Business Planning and Con... | Manual | SOX-ERP/GRC Role Review | Annually |
| IND0020096 | SOX-Database Review | SOX-SAP-11 Database changes | Manual | SOX-Database Review | Semi-annually |
| IND0020097 | SOX-SAP-05 Monthly High-Risk T-code Review | SOX-SAP-05 Monthly high-risk transaction... | Manual | SOX-High-Risk SAP Transaction Review | Monthly |
| IND0020098 | SOX-SAP-12 Monthly Transport Log Review | SOX-SAP-12 ERP transport audit log review | Manual | SOX-SAP Transport Log Review | Monthly |
| IND0020101 | SOX-Elevated User Role Review | SOX-ISA-04 Elevated/admin role review | Manual | SOX-Elevated User Role Review | Semi-annually |
| IND0020102 | SOX-SAP-13 SAP/BPC DR Test | SOX-SAP-13 ERP system server backup & re... | Manual | SOX-Disaster Recovery Test | Annually |
| IND0020105 | SOX-Elevated User Role Review on Subprod... | SOX-ISA-04 Elevated/admin role review | Manual | SOX-Elevated User Role Review on Subprod... | Semi-annually |
| IND0020111 | SOX-Segregation of Duties Review | SOX-SAP-03 Annual Segregation Of Duties ... | Manual | SOX-Segregation of Duties Review | Daily |
| IND0020112 | SOX-Update Set Change Review | SOX-ISA-01 Change review | Manual | SOX-Update Set Change Review | Quarterly |
| IND0020113 | SOX-Review of Database Accounts | SOX-SAP-14 Annual review of database acc... | Manual | SOX-Review of Database Accounts | Annually |
| IND0020243 | SOX-ITGC-01 Application change approvals | SOX-ISA-02 Application changes | Basic | SOX-Application Change Approvals | Monthly |

## Result

For information about the SOX Compliance Dashboard, see SOX Content Pack dashboard and reports.

### Verify the SOX Content Pack in Risk Management

After importing the SOX Content Pack, verify and edit the entity types, entities, risk statements, risks, and assessments within the Risk Management application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

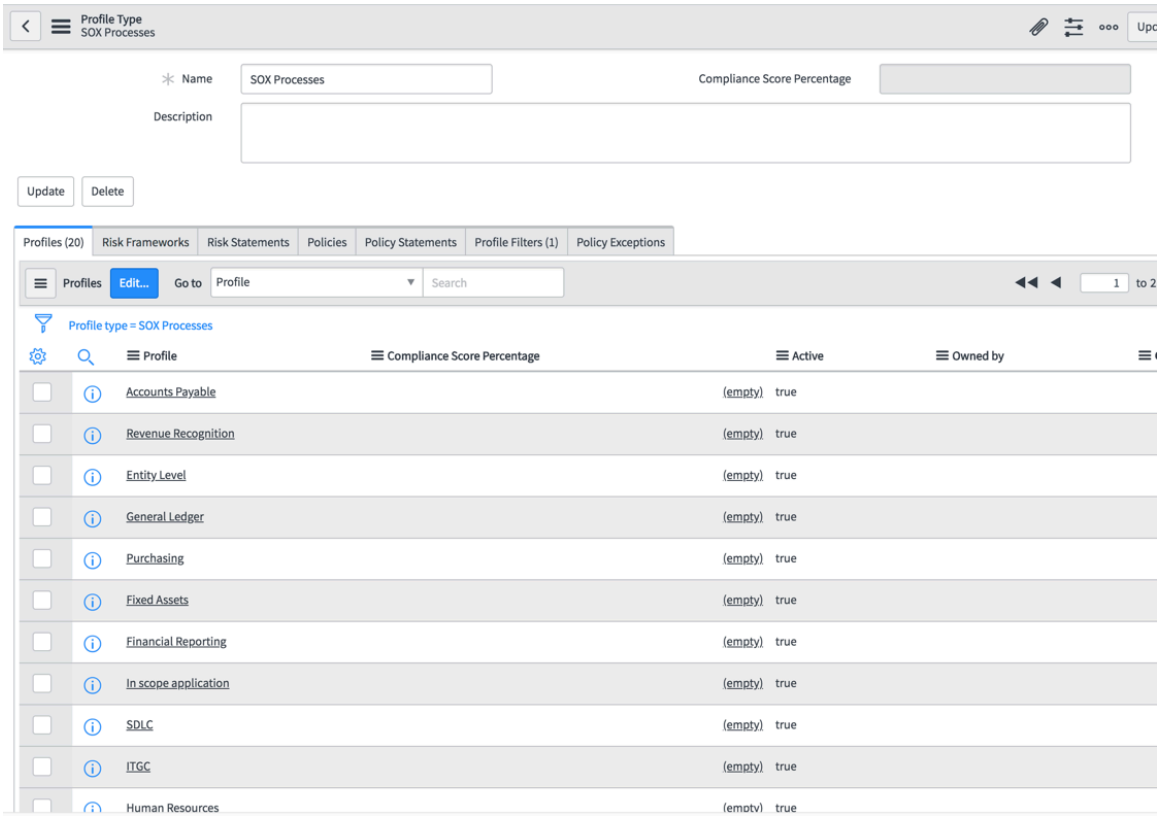
### Before you begin

Role required: Risk Admin (sn_risk.admin)

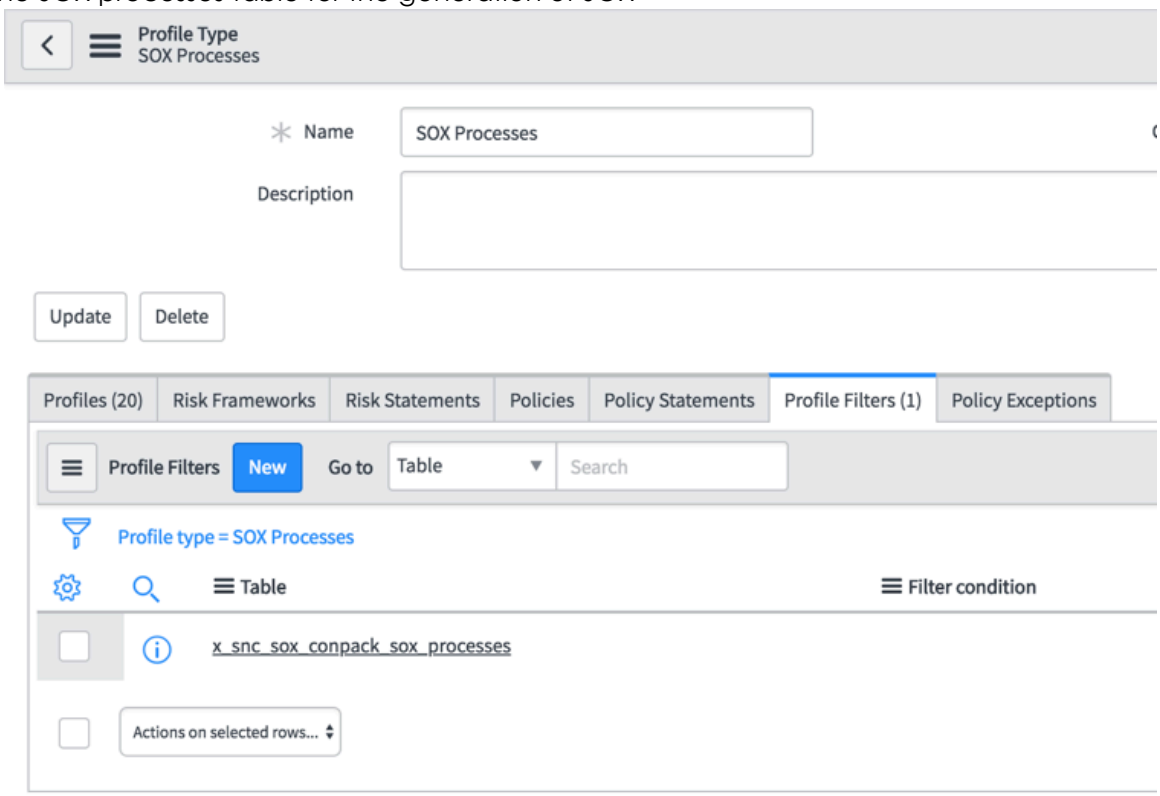
### Procedure

1. Navigate to **All** > **Risk** > **Scoping** > **Profile Type**.
   A **SOX Processes** entity type is added and is used to generate the SOX entities:
   - Accounts Receivable
   - Accounts Payable
   - Commissions
   - Equity
   - Entity Level
   - Financial Reporting
   - Fixed Assets
   - General Ledger
   - Human Resources
   - In Scope Application
   - Inventory
   - ITGC
   - Payroll
   - Purchasing
   - Revenue Recognition
   - SAP
   - SDLC
   - Tax
   - Travel and Expense
   - Treasury

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




2. Under the Profile filters related list, a filter is added to query the SOX processes table for the generation of SOX

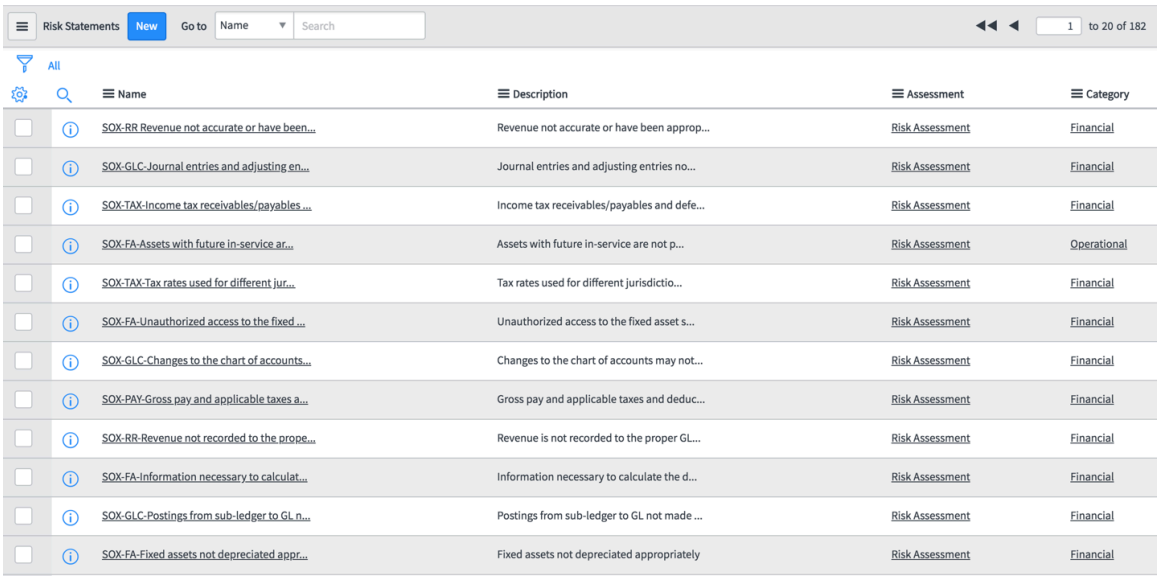



profiles.

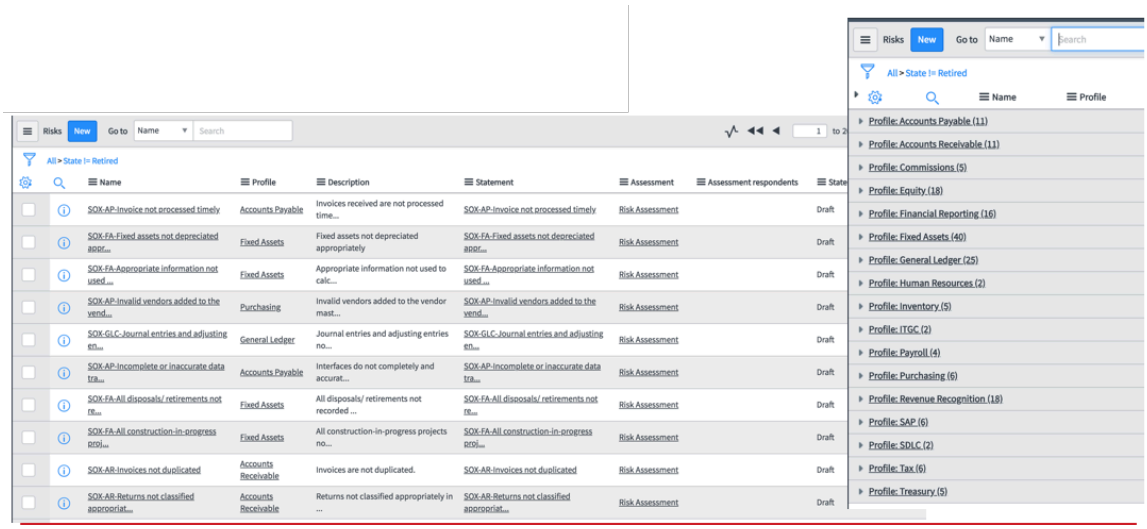
3. Navigate to **Risk** > **Risk Library** > **Risk Statements**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

All SOX risk statements have been added in the Draft state and the Risk Assessment is assigned to them.




4. Navigate to **Risk** > **Risk Register** > **Risks**.
   All SOX risk statements have been added in the Draft state and the Risk Assessment is assigned to them.




## Result

For information about the SOX Risk Dashboard, see SOX Content Pack dashboard and reports.

### Verify the SOX Content Pack in Audit Management

After importing the SOX Content Pack, verify and edit the entity types, entities, audit engagements, audit tasks, test templates, and test plans within the Audit Management application.

## Before you begin

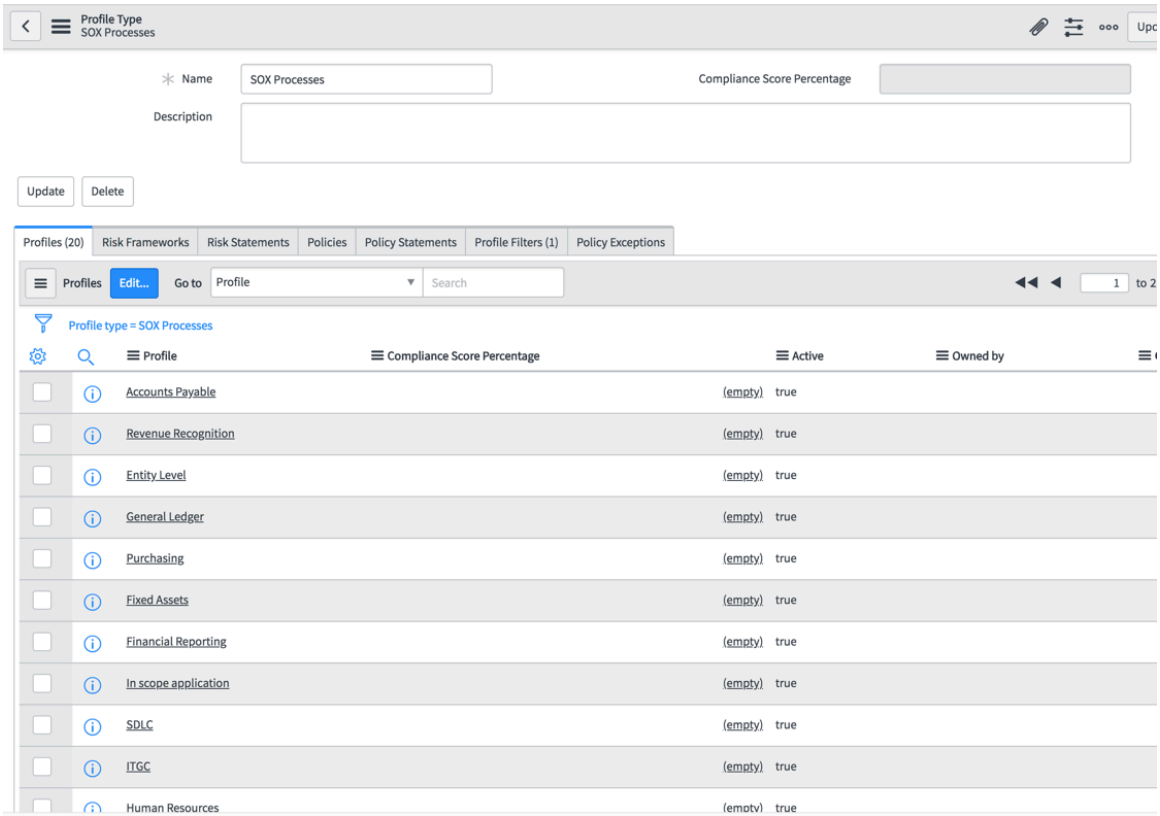
Role required: Audit Admin (sn_audit.admin)

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

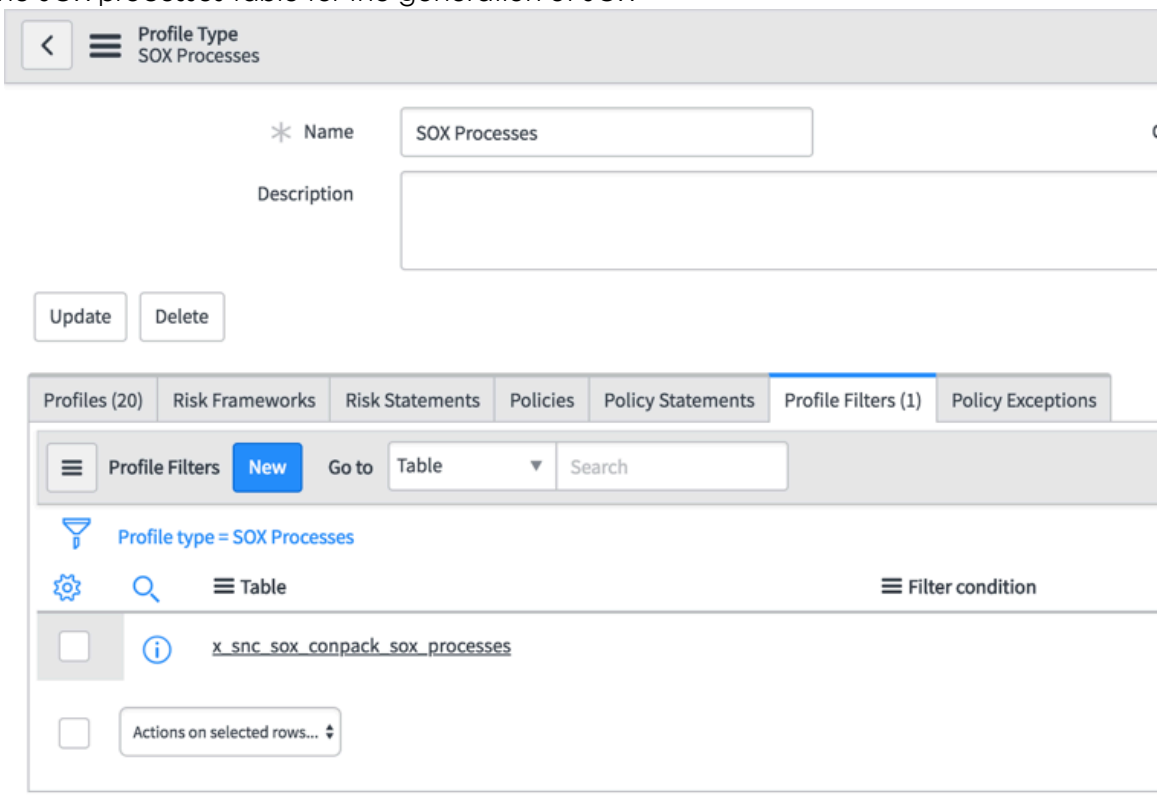
## Procedure

1. Navigate to **All** > **Audit** > **Entity Type**.
   A **SOX Processes** entity type is added and is used to generate the SOX entities:
   - Accounts Receivable
   - Accounts Payable
   - Commissions
   - Equity
   - Entity Level
   - Financial Reporting
   - Fixed Assets
   - General Ledger
   - Human Resources
   - In Scope Application
   - Inventory
   - ITGC
   - Payroll
   - Purchasing
   - Revenue Recognition
   - SAP
   - SDLC
   - Tax
   - Travel and Expense
   - Treasury

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




2. Under the Profile filters related list, a filter is added to query the SOX processes table for the generation of SOX



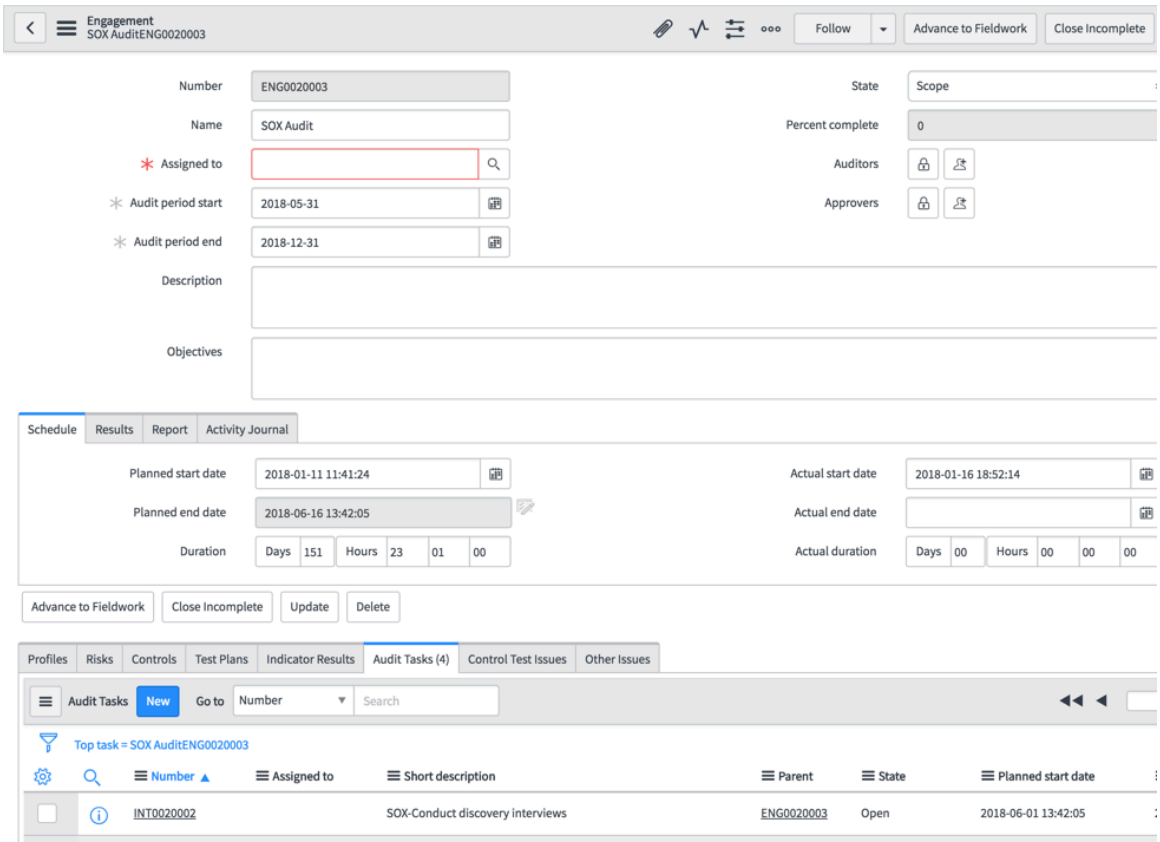

profiles.

3. Navigate to **Audit** > **All Engagements**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The **SOX Audit** engagement has been added in the Scope state with the following fields set as empty:

- **Assigned to**
- **Auditor**
- **Approver**

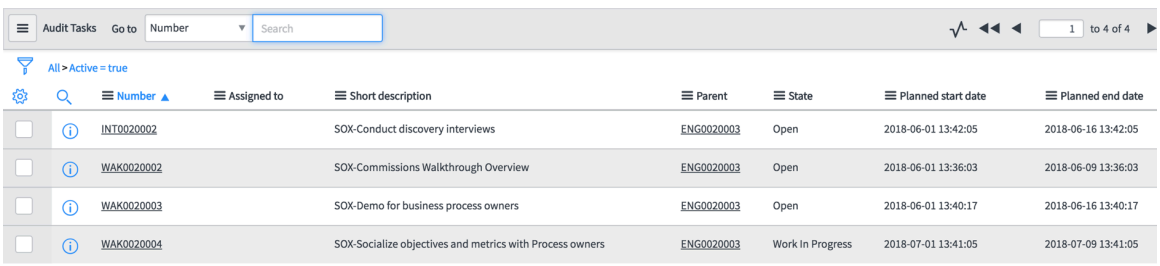



4. Navigate to **Audit** > **All Audit Tasks**.
5. In the search bar, enter `SOX` in the **Name** field.

> **Note:** The names of all SOX-related audit tasks start with **SOX**.

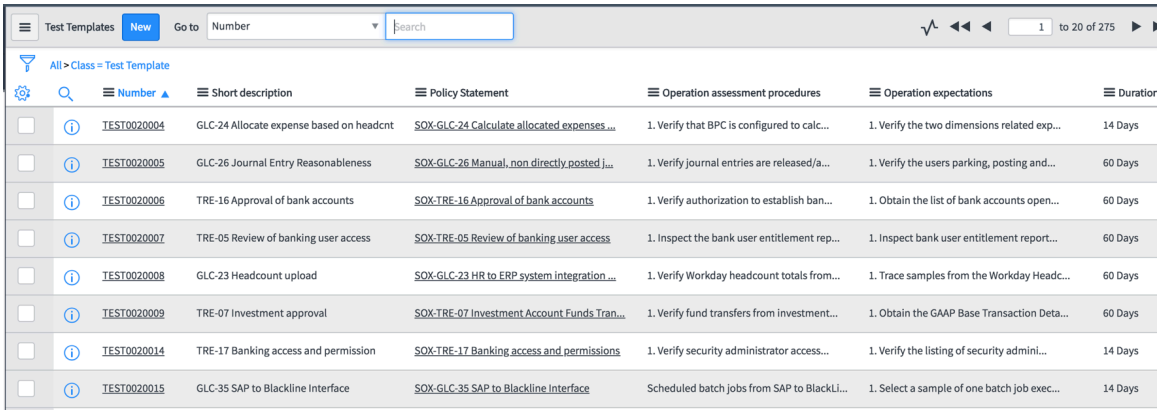
The SOX Audit tasks have been added with the following fields:

- **Type** is interview or walkthrough
- **Assigned to** is empty
- **Assigned parent (engagement)** is SOX Audit

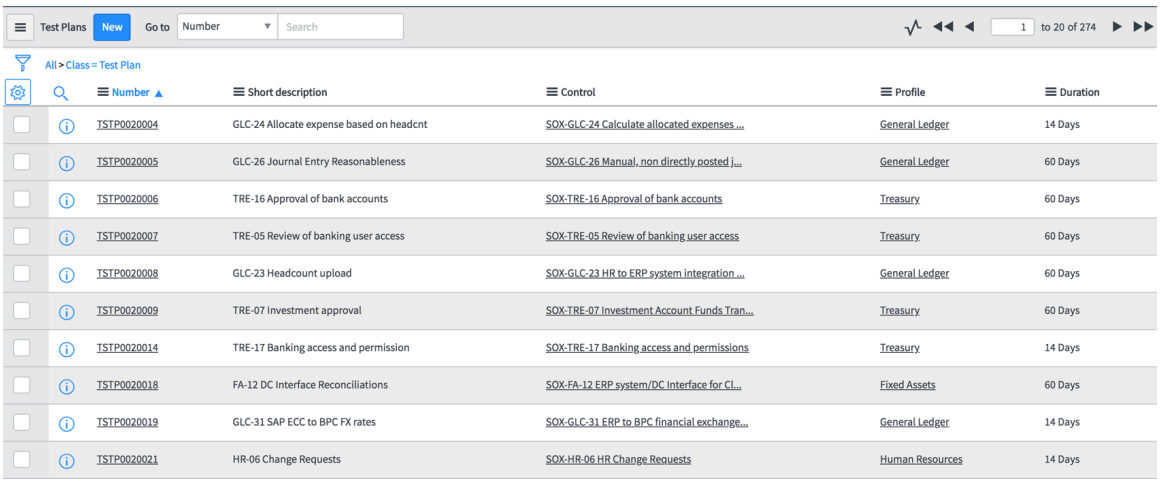



6. Navigate to **Audit** > **Audit Testing** > **Test Templates**.
   The SOX test templates have been added and assigned to policy statements.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




7. Navigate to **Audit** > **Audit Testing** > **Test Plans**.
   The SOX test plans have been generated for controls based on the test templates.




**Result**
For information about the SOX Audit Dashboard, see SOX Content Pack dashboard and reports.

### SOX Content Pack dashboard and reports

The SOX Content Pack dashboards display multiple SOX reports on a single screen. Various GRC roles have read or edit access to these dashboards.

## Policy and Compliance Management roles for SOX

- The Compliance Reader (sn_compliance.reader) can read **SOX Compliance Dashboard** and **SOX Processes**
- Compliance Manager (sn_compliance.manager) can read **SOX Compliance Dashboard**, **SOX Risk Dashboard**, and edit **SOX Processes**
- The Compliance Admin (sn_compliance.admin) can read **SOX Risk Dashboard** and edit **SOX Compliance Dashboard** and **SOX Processes**

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Risk Management roles for SOX

- Risk Reader (sn_risk.reader) can read **SOX Risk Dashboard** and **SOX Processes**
- Risk Manager (sn_risk.manager) can read **SOX Compliance Dashboard**, **SOX Risk Dashboard** and edit **SOX Processes**
- Risk Admin (sn_risk.admin) can read **SOX Compliance Dashboard** and edit **SOX Risk Dashboard** and **SOX Processes**

## Audit Management roles for SOX

- Audit User (sn_audit.user) can read **SOX Compliance Dashboard**, **SOX Risk Dashboard** and **SOX Processes**
- Audit Admin (sn_audit.admin) can read **SOX Compliance Dashboard**, **SOX Risk Dashboard** and edit **SOX Audit Dashboard** and **SOX Processes**

## SOX Compliance Dashboard

The SOX Compliance Dashboard displays an overview of all controls, attestations, and control issues. Navigate to **SOX** > **SOX Compliance Dashboard**. The following reports are available:

Compliance Overview

This dashboard shows the compliance overview of SOX policies and controls, and the effect on the entities related to SOX processes. It also shows:

- Key Controls
- Controls by Profile
- Control Compliance
- Controls by type
- Failed Controls
- Control Exceptions

Attestation Overview

This dashboard provides an overview of all the attestations related to SOX controls, and it helps to monitor the status and progress of attestations for the compliance teams to track. It shows:

- Pending Attestations
- Past due Attestations
- Attestations by Profiles
- My Attestations

Issue Overview

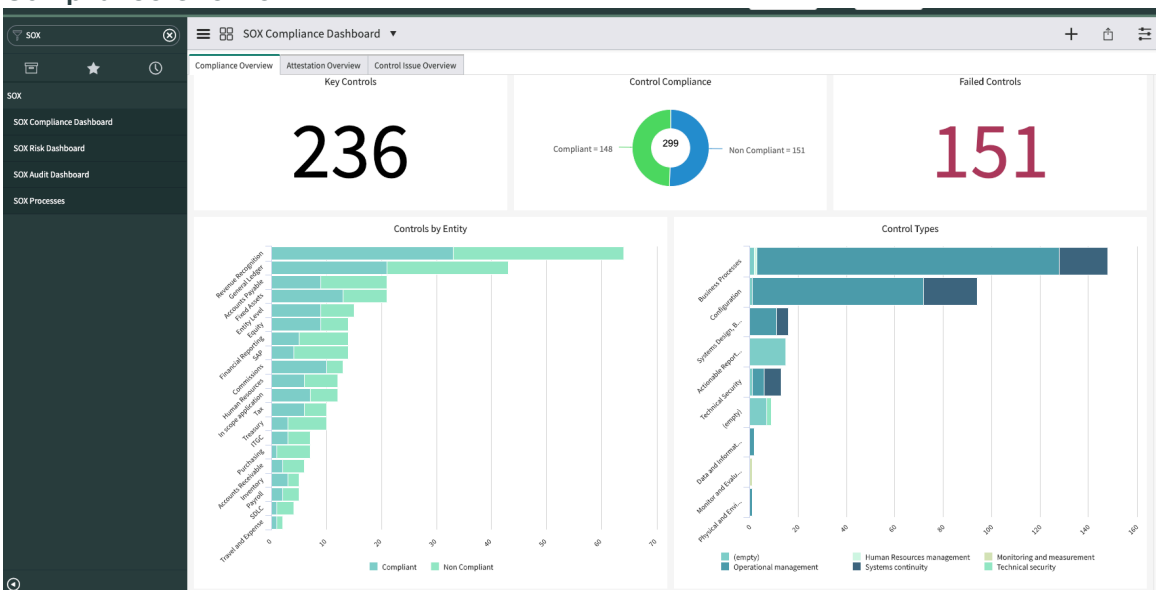
This dashboard provides an overview of all issues related to the SOX controls. It shows:

- Issues past due 90 days
- Issues pending 30 to 90 days
- Issues pending 30 days
- Issues due in next 30 days

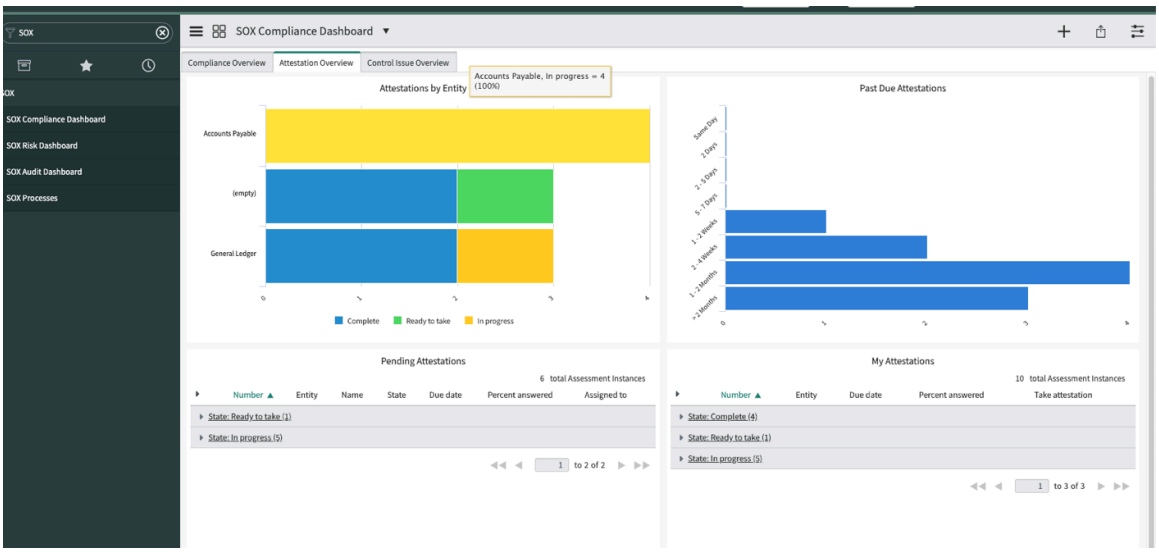
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Issues by Profile
- Pending Issues by Owner
- Issues Closure Rate
- Control Issues by Policy

## Compliance Overview

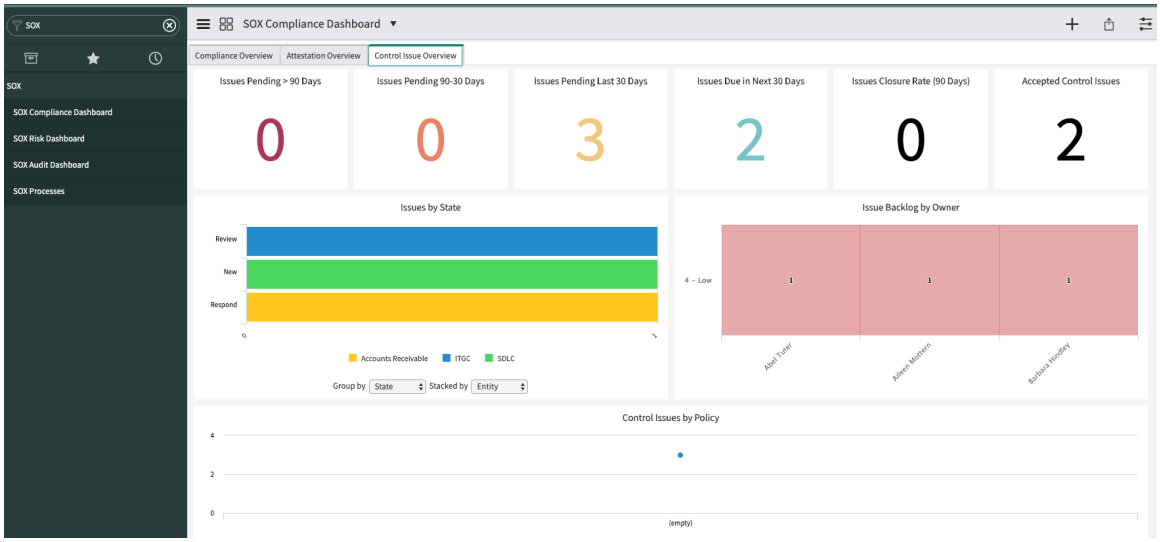



## Attestation Overview




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Control Issue Overview




## SOX Risk Dashboard

The SOX Risk Dashboard displays an overview of all risks, assessments, and risk issues. Navigate to **SOX** > **SOX Risk Dashboard**. The following reports are available:

Risk Overview

This dashboard provides an overview of the risks related to SOX processes and controls. It shows:

- Very high risk
- High risk
- Moderate risk
- Low risk
- Very low risk
- Risks by profile
- Risks by Response
- Inherent risk heatmap
- Residual risk heatmap
- Risks by Compliance
- Risk Exception

Assessment Overview

This dashboard provides the overview of the risk assessment for risks related to SOX processes and controls. It shows:

- Pending Assessments
- Past due Assessments
- Assessments by Profiles
- My Assessments

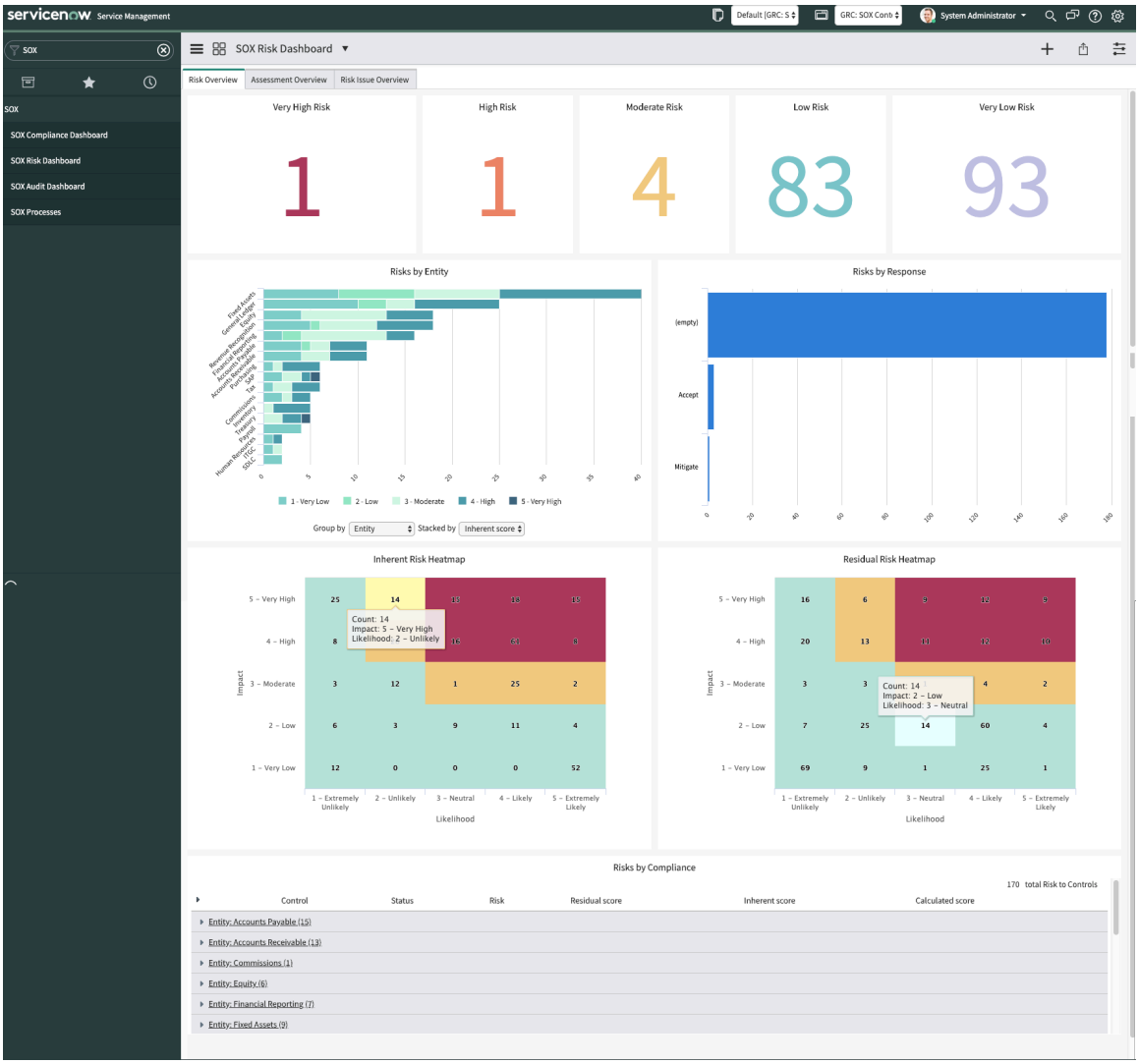
Issue Overview

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

This dashboard provides the overview of the risk issues related to SOX processes and controls, and helps the risk teams monitor the open issues that are assigned to the owners. It shows:

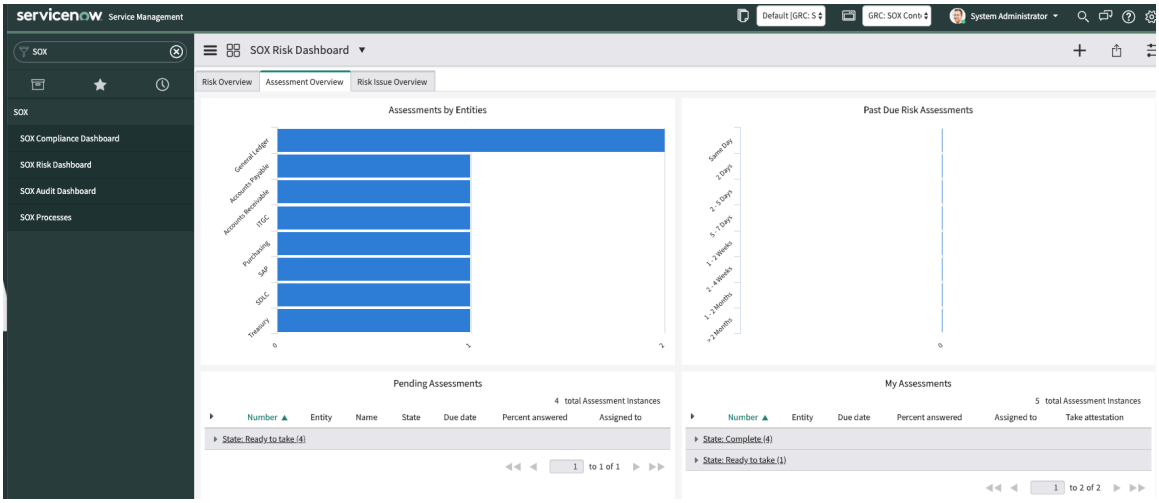
- Issues past due 90 days
- Issues pending 30 to 90 days
- Issues pending 30 days
- Issues due in next 30 days
- Issues by profile
- Pending Issues by Owner
- Issues Closure Rate
- Risks Issues by Policy

## Risk Overview

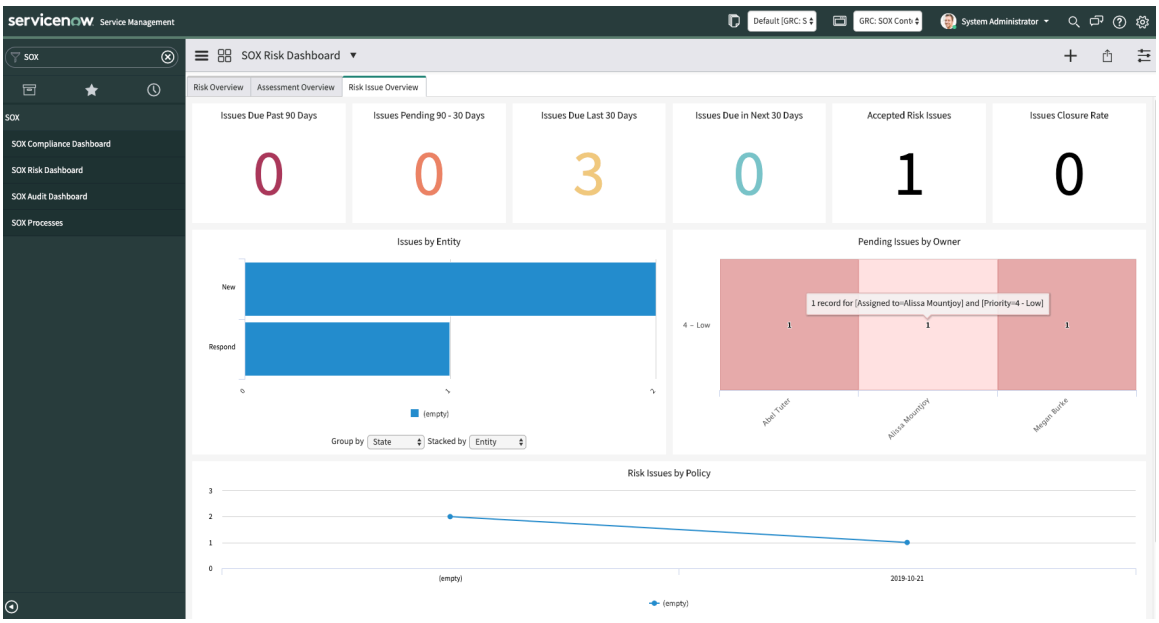



© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Assessment Overview




### Risk Issue Overview




## SOX Audit Dashboard

The SOX Audit Dashboard displays an overview of all audits and audit issues. Navigate to **SOX** > **SOX Audit Dashboard**. The following reports are available:

Audit Overview

This dashboard provides the progress of the ongoing SOX audits and monitors the various audit tasks. This is useful for the Audit managers. It shows :

- Audit Tasks Due > 90 Days
- Audit Tasks Due 90 to 30 Days
- Audit Tasks Due Last 30 Days
- Audit Tasks Due in Next 30 Days

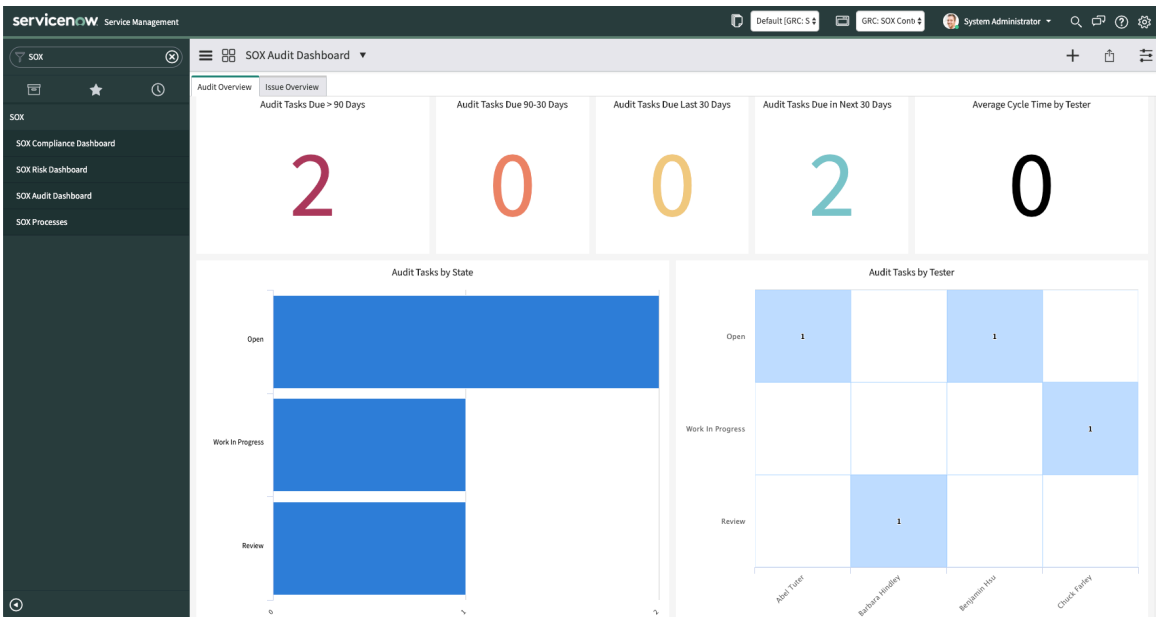
Issue Overview

This dashboard provides the progress of issues and helps audit teams to monitor the pending issues. It shows:

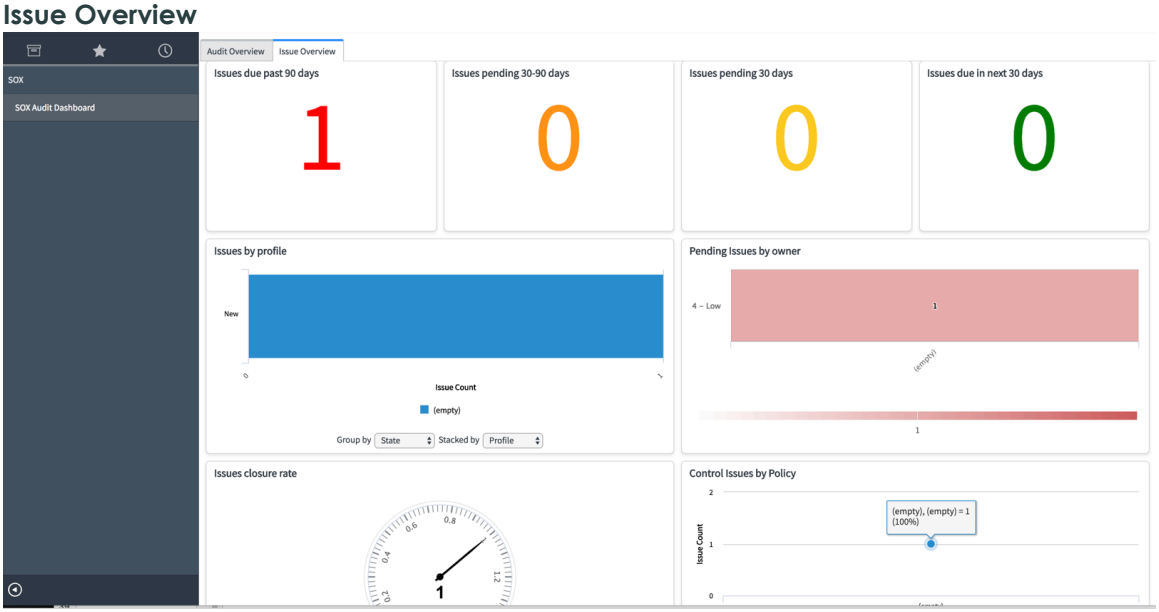
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Issues Due > 90 days
- Issues Due 30-90 days
- Issues Due Last 30 days
- Issues Due in Next 30 days
- Issues by profile
- Issues by Owner
- Pending Issues by Entity

### Audit Overview




### Issue Overview




## GRC integrations

Integrations enhance the ServiceNow® GRC product offering, providing users the ability to integrate with third-party applications.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use the following documentation for the installation, verification, and reporting features of the GRC integrations on the ServiceNow Store.

Unless otherwise noted, each integration requires that you have the ServiceNow GRC products installed and activated on your instance.

## GRC integration with Thomson Reuters Regulatory Intelligence

The ServiceNow® Regulatory Change Management application helps you to gather, monitor, and analyze regulatory data and track developments in a complex regulatory environment.

## Overview

Use the ServiceNow® GRC integration with Thomson Reuters Regulatory Intelligence application to integrate with the Thomson Reuters platform and to consume the Thomson Reuters Regulatory Intelligence (TRRI) feeds into your ServiceNow instance.

This integration helps you gather, monitor, and analyze regulatory data in a rapidly changing and complex regulatory environment. It enables you to efficiently manage and mitigate risks.

Thomson Reuters Regulatory Intelligence Integration (TRRI) delivers regulatory feeds that include various regulatory changes. The Regulatory Change Management application transforms and maps the feeds. The Regulatory Change Management application provides the information in regulatory feed tables.

With the Thomson Reuters guided setup, you can do the following:

- Receive regulatory feeds from the Thomson Reuters platform that are relevant to your organization.
- Transform and map the regulatory taxonomy from the Thomson Reuters platform to your internal regulatory taxonomy.
- Load the transformed data into your ServiceNow instance and manage regulatory changes.

In the guided setup, you can do multiple tasks and subtasks:

- Create a Connection: Create a connection and validate it. The connection is required for integration with the Thomson Reuters platform. Tasks in this step include the following:
  - Create Connection
  - Validate Connection
  - Submit OAuth Credentials
- Activate Integration Flows: Set up a schedule and activate the flows at different times. Run the flows with a time gap, such as a gap of 12 hours between the flows. Tasks in this step include the following:
  - Configure the flow that inserts feed files into the feed registry.
  - Configure the flow that moves processed feeds into the destination directory.
- Create an Internal Taxonomy: Create your taxonomy to categorize and classify the regulatory content. An internal taxonomy can be a multi-hierarchical structure.
- Map an External Taxonomy to an Internal Taxonomy: Map the source taxonomy from the Thomson Reuters platform with the internal taxonomy that you have created.

When setting up the integration, you go through the following stages:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. Configure feed settings: Configure and set up the feed content, delivery settings, and delivery location in the Thomson Reuters Regulatory Intelligence (TRRI) feeds platform. The delivery location is where the feeds are delivered.
2. Set up a MID Server: The Thomson Reuters platform sends the regulatory feed files to the SFTP server that's configured on the Thomson Reuters portal. An administrator should set up a MID Server with SSH capabilities for the GRC integration with Thomson Reuters Regulatory Intelligence application.

   The MID Server ingests the feed file data from the SFTP server into the ServiceNow instance. The MID Server runs as a Windows service or as a UNIX daemon to facilitate communication between an instance and the external applications.
3. Set up SFTP connection: The Thomson Reuters platform deposits the regulatory feed files at an SFTP location that is configured in the Thomson Reuters platform portal. Create an SFTP connection and import the feed files into your ServiceNow instance. To learn more, see Establish an SFTP or REST API connection.

Import sets enable administrators to import data from various data sources, and then map that data into ServiceNow tables.

## Bringing series data from Thomson Reuters into the Regulatory Change Management application

The Documents in Series related list enables you to track the development of a regulatory change from the proposed stage to the final stage. You can see related events in a single place. In the Regulatory Feed form, the series name, and the regulatory events that are part of the Thomson Reuters series are displayed. You can view the Thomson Reuters series data in the Series Data section in the Regulatory Feed form. The series name and the sequence number of the feed are displayed under the Series Data section in the Regulatory Feed form. This section helps you to get more context on the regulatory events and to make decisions regarding the applicability of the events.

The Regulatory Feed table appears in the Series Data section in the Regulatory Feed form. The following new columns are added to the Regulatory Feed table for the Thomson Reuters series data:

- Series Name: Displays the series name of the regulatory event.
- Sequence Number: Displays the sequence number of the regulatory event.
- Series ID: Displays the series identification number of the regulatory event. You can select the series ID from the list view. The series ID is then displayed.

The Documents in Series related list is part of the regulatory feed form. It displays the following details on the feed:

- Number: The number of the regulatory feed as received from Thomson Reuters. For example, REG0001023.
- Title: The title of the regulatory feed as received from Thomson Reuters. For example, CFPB-2019-0021 Home Mortgage Disclosure (Regulation C).
- Sequence Number: The sequence number of the regulatory feed as received from Thomson Reuters. For example, sequence number 7. If you have all the data, then the prior six events are displayed in the related list and the seventh event in the series is displayed.

**Note:** The Series Data section and the Documents in Series related list are displayed in the Regulatory Feed form only if the feed type is regulatory event and the source of the regulatory feed is Thomson Reuters.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The regulatory data that is received from the Thomson Reuters platform is processed and brought into the staging tables in a ServiceNow instance.

## Actions to automate the integration tasks

The GRC integration with Thomson Reuters Regulatory Intelligence application provides the following actions to automate the Thomson Reuters integration tasks:

- Get the related source documents for the regulatory events.
- Get the Thomson Reuters platform to feed file names from the SFTP source path.
- Move the files processed by the Thomson Reuters platform to the destination path.
- Trigger the scheduled import job in the Thomson Reuters platform after getting the file names from the SFTP server.
- Validate the path and credentials for the new SFTP connection.

The instructions for automation are covered in detail in the guided setup files that are sent with the software.

### Install the GRC integration with Thomson Reuters Regulatory Intelligence application

Install the GRC integration with Thomson Reuters Regulatory Intelligence application (com.sn_grc_int_tr). The application includes demo data. It installs related ServiceNow Store applications and plugins if they are not already installed.

#### Before you begin

- Ensure that the application and all of its associated ServiceNow Store applications have valid ServiceNow entitlements. For more information, see Get entitlement for a ServiceNow product or application.

The GRC integration with Thomson Reuters Regulatory Intelligence requires the ServiceNow® Regulatory Change Management application from the ServiceNow Store. Ensure that this application is installed before you install the GRC integration with Thomson Reuters Regulatory Intelligence application.

Role required: sn_grc_reg_change.admin

#### About this task

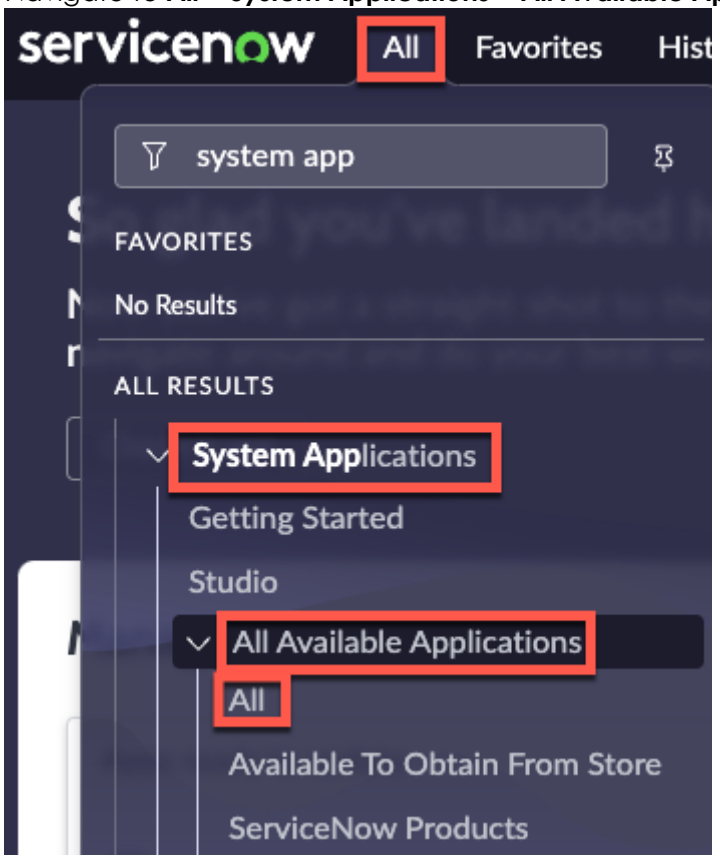
The following items are installed with the GRC integration with Thomson Reuters Regulatory Intelligence application:

- Store applications
- Scheduled jobs
- Tables

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **System Applications** > **All Available Applications** > **All**.




2. Find the GRC integration with Thomson Reuters Regulatory Intelligence application (com.sn_grc_int_tr) by using the filter criteria and search bar.

   You can search for the application by its name or ID. If you cannot find the application, then you might have to request it from the ServiceNow Store.

   Visit the ServiceNow Store website to view all the available apps and for information about submitting requests to the store. For cumulative release notes information for all released apps, see the ServiceNow Store version history release notes.

3. In the Application installation dialog box, review the application dependencies.

   Dependent plugins and applications are listed if they will be installed, are currently installed, or need to be installed. If any plugins or applications need to be installed, then you must install them before you can install the GRC integration with Thomson Reuters Regulatory Intelligence application.

4. Select **Install**.

#### Establish an SFTP or REST API connection

Establish an SFTP or REST API connection for the GRC integration with Thomson Reuters Regulatory Intelligence application. You can create an SFTP or REST API connection with the SFTP server by using the Connection & Credential aliases that are shipped with the Thomson Reuters platform.

### Before you begin

Role required: sn_grc_reg_change.admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

Thomson Reuters deposits the regulatory feed files at the SFTP location that is configured in Thomson Reuters portal. To import the feed files from the SFTP location into the ServiceNow instance, you can create a connection with this SFTP server.

### Procedure

1. Navigate to **All** > **Regulatory Change Management** > **Thomson Reuters** > **Connection & Credential Aliases**.
   The following two Connection & Credential aliases are shipped with the Thomson Reuters platform:
   - The Thomson Reuters platform REST API
   - The Thomson Reuters platform SFTP
2. In either the Thomson Reuters platform REST API alias or the Thomson Reuters platform SFTP alias, click the **Create New Connection & Credential** related link.
   You can create a connection with either the REST alias or the SFTP alias, but not both. The details to be provided in the SFTP alias and the REST alias are different from each other. When you enter the details in the Create Connection & Credential alias form, a new connection is created.
3. On the form, fill in the fields.
   - If you selected the Create Connection & Credential SFTP alias form, then fill in the following fields.

**Create Connection & Credential SFTP alias form**

| Field | Description |
|---|---|
| Connection information | |
| Name | Name of the SFTP connection. |
| Host | Information about the SFTP server host. |
| Port | Port number of the SFTP server. |
| Credential information | |
| Name | Credential name that is used to access the SFTP server. |
| User Name | User name that is used to access the SFTP server. |
| Password | Password that is used to access the SFTP server. |
| Post processing information | |
| Source path | Location of the directory that contains the regulatory feed files. |
| Destination path | Location of the directory where the successfully imported files are placed. |

   - If you selected the Create Connection & Credential REST alias form, then fill in the following fields.

**Create Connection & Credential REST alias form**

| Field | Description |
|---|---|
| Credential information | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| OAuth client ID | Client ID of the application that is registered in the third-party OAuth OIDC server. |
| OAuth client secret | Client secret ID of the application that is registered in the third-party OAuth OIDC server. |

4. Depending on your previous step, click either **Create** in the SFTP alias form or click **Create and Get OAuth Token** in the REST alias form.
   The File Connection Information record is created.

**Result**
When a new connection is established, a file connection information record is created in the instance. After the file connection information record is created, you can no longer create more file connection information records by clicking **New** in the Connections related list.

### Modules in the GRC integration with Thomson Reuters Regulatory Intelligence application

The GRC integration with Thomson Reuters Regulatory Intelligence application includes various modules.

The following modules are displayed under the GRC integration with Thomson Reuters Regulatory Intelligence application:

#### Modules in the application

| Module | Description |
|---|---|
| Thomson Reuters Guided Setup | Instructions to configure and set up the application. |
| Connection & Credential Aliases | Connection and credential aliases for SFTP and for OAuth. |
| Connections | File connection information record from the Thomson Reuters platform. Click Validate to validate the connection. In case you encounter any issues in validating the connection, triage it using an integration log.<br><br>If you do not want to use a connection, you can move it to the Draft state by clicking **Move to draft**. In the integration, the system uses only the file connection information record that has the Validated state. |
| OAuth Registry Entry | Record of when the OAuth connection and credential are created via the shipped connection and credential alias. |
| OAuth Credentials | Record of when the OAuth credentials are created. |
| Feed Registry | Record for each of the feed files that are located in the source directory of the SFTP location. |
| Integration Logs | Integration logs with integration details. The log contains errors that occurred in the integration |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Modules in the application (continued)**

| Module | Description |
|---|---|
| | flows, such as, errors that were observed while validating a connection. |
| Data source | Data source that ingests the feed files from the SFTP location and creates a record automatically in the regulatory feed table. |
| Scheduled Import | Scheduled import job that scans and searches for the oldest entry in the feed registry. |
| Taxonomy XML Configuration | Record that is shipped as part of the Thomson Reuters platform. Contains the XPaths and attributes that are required to parse the uploaded Thomson Reuters platform taxonomy file in XML format. |
| TR \| Regulatory Bodies | External Regulatory Bodies taxonomy records for the Thomson Reuters platform. |
| TR \| Content Types | External Content Types taxonomy records for the Thomson Reuters platform. |
| TR \| Jurisdictions | External Jurisdictions taxonomy records for the Thomson Reuters platform. |
| TR \| Themes | External Themes taxonomy records for the Thomson Reuters platform. |
| TR \| Sectors | View the external Sectors taxonomy records for the Thomson Reuters platform. |
| Taxonomy Mapper | Mapping of the Thomson Reuters platform taxonomy to internal taxonomy. |

The data that is accessed through the application modules is stored in the following tables:

**Tables for storing application data**

| Table | Field |
|---|---|
| sn_grc_reg_change_external_theme | External Regulatory Theme |
| sn_grc_reg_change_external_regulatory_body | External Regulatory Body |
| sn_grc_reg_change_external_sector | External Regulatory Sector |
| sn_grc_reg_change_external_content_type | External Regulatory Content Type |
| sn_grc_reg_change_external_jurisdiction | External Regulatory Jurisdiction |
| sn_grc_reg_change_ theme | Regulatory Theme |
| sn_grc_reg_change_ regulatory_body | Regulatory Body |
| sn_grc_reg_change_sector | Regulatory Sector |
| sn_grc_reg_change_ content_type | Regulatory Content Type |
| sn_grc_reg_change_ jurisdiction | Regulatory Jurisdiction |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

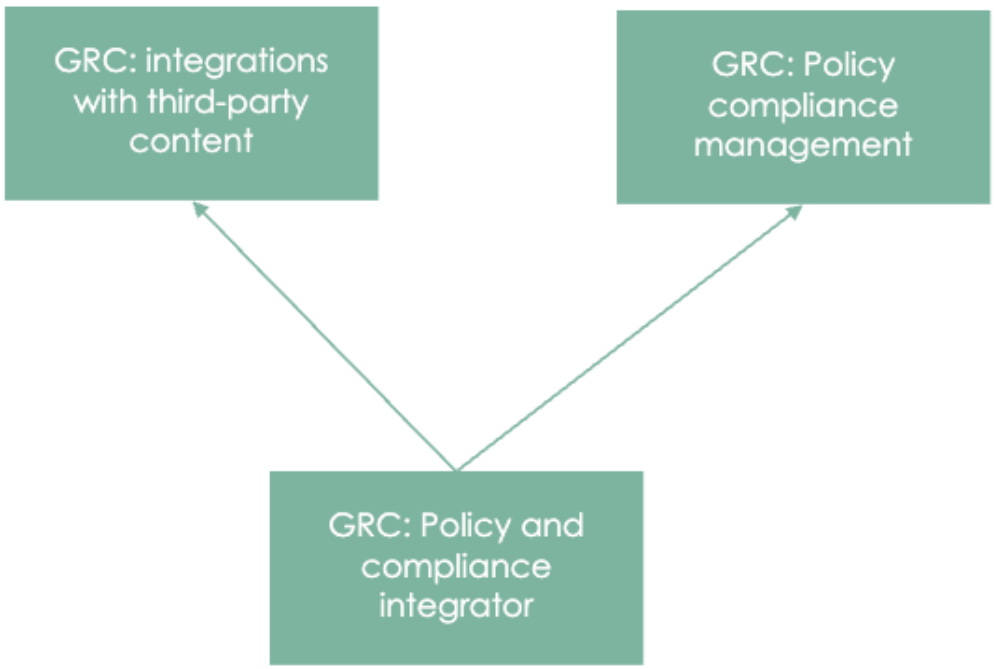
## GRC: integrations with third-party content

The GRC: integrations with third-party content application helps you to standardize the content integration process across various GRC applications by providing a common framework for your content providers.

In Utah, you can use the GRC: integrations with third-party content application with the GRC: Policy and Compliance integrator application. The GRC: Policy and Compliance integrator application provides the options that enable you to review, approve, and import the data into the Policy and Compliance Management tables.

You can install the GRC: integrations with third-party content application separately from the ServiceNow Store. When you download the GRC: Policy and Compliance integrator application from the ServiceNow Store, the GRC: integrations with third-party content application is downloaded automatically in your instance as shown in the following diagram.

**GRC: Policy and Compliance integrator application download structure**




**Note:** The GRC: integrations with third-party content application is not visible in the application navigator in an instance.

When the GRC: integrations with third-party content and GRC: Policy and Compliance integrator applications are downloaded in your instance, a user with the sn_grc_cim.admin role can execute the tasks that are related to the application workflow.

For more information on the user roles, see User roles for the integration process and Create a user with the sn_grc_cim.admin role.

### User roles for the integration process

You must assign the user roles that are required for the overall integration process that is associated with the GRC: integrations with third-party content and GRC: Policy and Compliance integrator applications.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

You can assign the following roles with the GRC: integrations with third-party content and GRC: Policy and Compliance integrator applications.

**User roles**

| Role titles | Description |
|---|---|
| sn_grc_cim.admin | As a user with the sn_grc_cim.admin role, you can access the APIs and the tables in the GRC: integrations with third-party content application. |
| sn_grc_cim.manager | As a user with the sn_grc_cim.manager role, you have read and write access to the tables in the GRC: integrations with third-party content application. |
| sn_compliance.manager | The sn_compliance.manager role inherits the sn_grc_cim.manager role. As a user with the sn_compliance.manager role, you have read and write access to the tables in the GRC: Policy and Compliance Management application. |
| sn_compliance.admin | The sn_compliance.admin role inherits the sn_grc_cim.admin role. As a user with the sn_compliance.admin role, you can access the tables in the GRC: Policy and Compliance Management application. |

### Create a user with the sn_grc_cim.admin role

Create a user with the sn_grc_cim.admin role to perform the tasks that are related to the content integration and import process.

#### Before you begin

**Note:** Ensure that you have installed the GRC: integrations with third-party content application in your instance. For more information, see GRC: integrations with third-party content.

Role required: sn_grc_cim.admin, sn_compliance.admin

#### Procedure

1. Log in to an instance with the sn_compliance.admin role and assign the sn_grc_cim.admin role to a user.

   **Note:** The sn_compliance.manager role inherits the sn_grc_cim.manager role. Similarly, the sn_compliance.admin role inherits the sn_grc_cim.admin role.

   As a user with the sn_grc_cim.admin role, you can access all the APIs that are required to insert the records into the GRC: integrations with third-party content application. As a user with the sn_grc_cim.manager role, you have the write access to the tables of the GRC: integrations with third-party content application.

2. Navigate to the GRC: Policy and Compliance integrator application in an instance to execute the workflow.
   For the next steps that you must do in the GRC: Policy and Compliance integrator application workflow, see Workflow for GRC: Policy and Compliance integrator.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Standardized Information Gathering (SIG) Questionnaire Integration

The Shared Assessments Standardized Information Gathering Questionnaire (SIG) is used to obtain required assessment documentation from a third party. The third-party contact can upload a pre-filled SIG spreadsheet or take a form-based questionnaire that is imported to the instance.

## Supported SIG versions

TPRM supports the current SIG version and two prior versions.

- SIG Full 2023, 2022, 2021
- SIG Core 2023, 2022, 2021
- SIG Lite 2023, 2022, 2021

## Uploading SIG data

- If a third party uploads a version prior to the earliest supported SIG, all responses for matching questions are imported and any non-matching questions are imported with blank responses for the third party to answer later.
- If a third party attempts to load data from a version of SIG that is older than the current version, some questions might not be mapped or parsed correctly (for example, if you load data for SIG 2022 full on SIG 2023 full).

Related topics

Install the GRC: SIG Questionnaire Integration

Verify the SIG Questionnaire Integration in Vendor Risk Management

### Install the GRC: SIG Questionnaire Integration

The GRC: SIG Questionnaire plugin installs the supported questionnaire templates for use with the GRC: TPRM application.

**Before you begin**
Role required: sn_vdr_risk.admin, admin
Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation.

| Setup task | Description |
| --- | --- |
| Verify that the ServiceNow plugins are activated. | Activate the Vendor Risk Management (com.sn_vdr_risk_asmt) plugin.<br><br>To verify that this plugin is activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased.<br><br>For more information about the setup and activation of the GRC Vendor Risk Management plugin, see Configuring Third-party Risk Management. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Log in to the instance you want to install the application on.
2. Navigate to **System Applications** > **All Available Applications** > **All**.
   A list of apps available for installation is displayed.
3. Locate the app, select it, and click **Install**.
   The app installs GRC: Vendor Risk Management (com.sn_vdr_risk_asmt) plugin and GRC: SIG Assessment Core (com.snc.sig_asmt_core) plugin.

> **Note:** When uninstalling the app, select the check box to retain the profile types profiles and indicators.

## Verify the SIG Questionnaire Integration in Vendor Risk Management

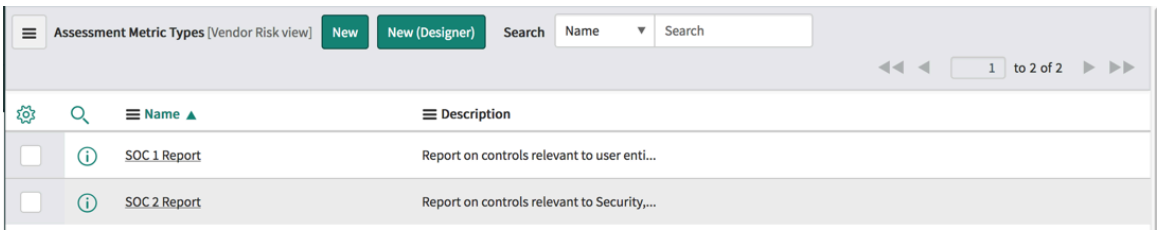
After installing SIG Questionnaire Integration, verify questionnaire templates, document request templates, and assessment templates within the Vendor Risk Management application.

### Before you begin

Role required: Vendor Risk Manager (sn_vdr_risk_asmt.vendor_risk_manager)

### Procedure

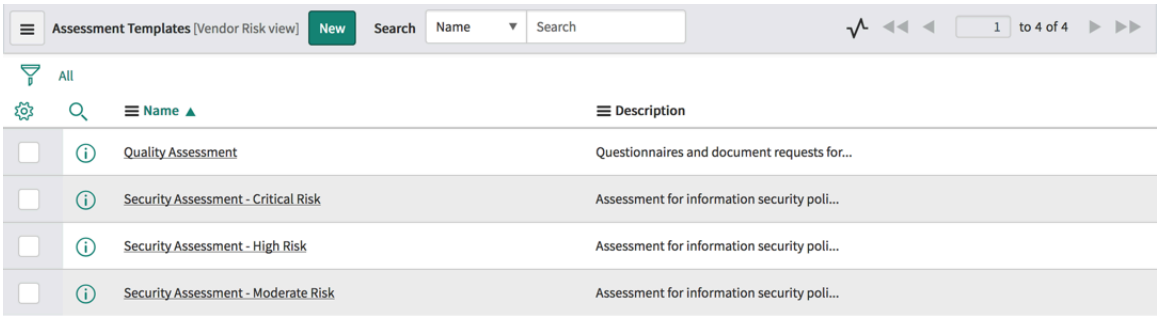
1. Navigate to **All** > **Vendor Risk Management** > **Assessment Setup** > **Questionnaire Templates**.
   The supported questionnaires are added.
2. Navigate to **Vendor Risk Management** > **Assessment Setup** > **Document Request Templates**.
   The following questionnaires are added:
   - SOC 1 Report
   - SOC 2 Report




3. Navigate to **Vendor Risk Management** > **Assessment Setup** > **Assessment Templates**.
   The following templates are added:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Security Assessment — Critical Risk
- Security Assessment — High Risk
- Security Assessment — Moderate Risk




Related topics

Standardized Information Gathering (SIG) Questionnaire Integration

## GRC use case accelerators

Use case accelerators may include pre-defined scopes, specific policies, controls, risks, audit, test plans, dashboards, and reports that provides customers an operational head-start when adopting various regulations and frameworks.

Use the following documentation for the installation, verification, and reporting features of the GRC use case accelerators on the ServiceNow Store.

Unless otherwise noted, each use case accelerator requires that you have the ServiceNow GRC products installed and activated on your instance.

### Cybersecurity Controls Accelerator

The Cybersecurity Controls Accelerator™ enables users to easily adopt the CIS Controls from The Center for internet Security™ to enhance their overall security preparedness and cyber-defense posture.

CIS Control adoption is further enhanced by targeting the leading cybersecurity methodologies to the user's maturity and readiness level.

The Cybersecurity Controls Accelerator contains the CIS Controls version 7.1 authority document, 191 associated CIS citations, and 191 CIS control objectives that are related to the citations.

The Technology Controls Monitoring Accelerator application (com.sn_grc_infosec), which must also be downloaded to use the Cybersecurity Controls Accelerator, includes 171 (26 basic) predefined indicator templates that are mapped to the CIS Controls. These indicator templates provide automated control validation and continuous monitoring.

### Support for CIS Controls™ v8

Beginning with the Utah release, Cybersecurity Controls Accelerator supports CIS Controls™ v8 authority documents, citations, and control objectives that are related to the citations.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Content for CSA CCM v4.0

Beginning with the Utah release, Cybersecurity Controls Accelerator supports the Cloud Security Alliance Cloud Controls Matrix (CSA CCM v4.0) content such as Authority Document, Citations, and Control Objectives.

### Download the Cybersecurity Controls Accelerator

Before you run the GRC: Cybersecurity Controls Accelerator application in your instance, you must download it from the ServiceNow Store.

#### Before you begin

Prior to running the Cybersecurity Controls Accelerator application, you must download and activate the following GRC applications:

- GRC: Policy and Compliance Management
- GRC: Profiles
- GRC: Technology Controls Monitoring Accelerator

Role required: admin

#### Procedure

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

### Monitoring cybersecurity controls

After you have accessed the Cybersecurity Controls Accelerator, you can monitor the controls using these modules.

**Cybersecurity Controls Accelerator modules**

| Application/ Module | Description |
|---|---|
| **CIS Controls** | |
| Authority Documents | The **Authority Documents** module provides a list of authority documents, including the CIS Controls v7.1 and v8 authority documents. The authority documents include references to citations and control objectives.<br><br>The authority documents are stored in the Authority Document table [sn_compliance_authority_document]. |
| Citations | The **Citations** module provides a list of citations contained in the CIS Controls v7.1 and v8 authority document. Each citation can include one or more control objectives and refers to:<br>• Content references<br>• Information objects<br><br>The citations are stored in the Citation table [sn_compliance_citation]. |
| Control Objectives | The **Control Objectives** module provides a list of control objectives associated with the citations in the CIS Controls v7.1 and v8 authority document. Each control objective can include one or more of the following items: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Cybersecurity Controls Accelerator modules (continued)**

| Application/ Module | Description |
|---|---|
| | • Entity types<br>• Additional entities<br>• Policies<br>• Controls<br>• Indicator Templates<br>• Policy Exceptions<br>• Issues<br>• Risk statements<br>• Content references<br><br>The control objectives are stored in the Control Objective table [sn_compliance_policy_statement] |
| Indicator Templates | The **Indicator Templates** module provides a list of predefined indicator templates that are mapped to the CIS Controls. The indicator templates automate control validation and provide continuous monitoring.<br><br>Indicator Template Reference to Content [sn_grc_m2m_ind_temp_cont] |

As previously mentioned, the Technology Controls Monitoring Accelerator application (com.sn_grc_infosec) is a dependant application when you download the Cybersecurity Controls Accelerator application. The Technology Controls Monitoring Accelerator application provides predefined indicator templates that are mapped to the CIS Controls.

**Note:** Should you decide not to implement the Cybersecurity Controls Accelerator application, you can still use the Technology Controls Monitoring Accelerator to validate compliance with CIS and ISO 27002 via the Unified Compliance Framework (UCF) from the Policy and Compliance Management application. For more information, see Technology Controls Monitoring Accelerator.

### UCF controls mapped to indicator templates

If you use the CIS or ISO authority documents imported from UCF, you can still manage compliance activities using the 285 (171 CIS and 114 ISO) automatically monitored indicator templates.

The 171 indicator templates are mapped to the 171 CIS control objectives provided with the Cybersecurity Controls Accelerator application.

**Note:** the information in the 26 basic indicator templates is drawn from various ServiceNow ITx applications, as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Basic indicator templates for CIS Controls

| CIS Control | Description | ITx Source applications |
|---|---|---|
| CIS Control 1.1 | Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory. | Discovery |
| CIS Control 1.2 | Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory. | Discovery |
| CIS Control 1.4 | Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not. | Discovery |
| CIS Control 1.5 | Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network. | Discovery |
| CIS Control 1.6 | Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner. | Discovery |
| CIS Control 1.7 | Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network. | Discovery |
| CIS Control 1.8 | Use client certificates to authenticate hardware assets connecting to the organization's trusted network. | Discovery |
| CIS Control 2.1 | Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system. | Software Asset Management |
| CIS Control 2.2 | Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system. | Software Asset Management |
| CIS Control 2.3 | Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems. | Software Asset Management |
| CIS Control 2.4 | The software inventory system should track the name, version, publisher, and installation date for all software, including operating systems authorized by the organization. | Software Asset Management |
| CIS Control 2.5 | The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location. | CMDB |
| CIS Control 3.1 | Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or | Vulnerability Response |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

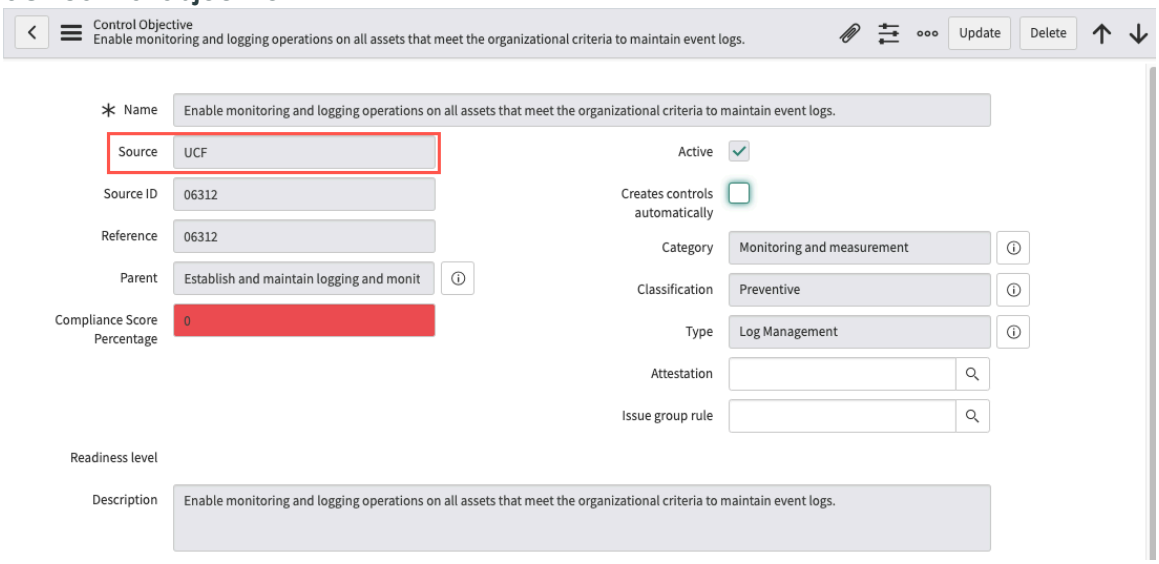
### Basic indicator templates for CIS Controls (continued)

| CIS Control | Description | ITx Source applications |
|---|---|---|
| | more frequent basis to identify all potential vulnerabilities on the organization's systems. | |
| CIS Control 3.2 | Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested. | Vulnerability Response |
| CIS Control 3.6 | Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner. | Vulnerability Response |
| CIS Control 3.7 | Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities. | Vulnerability Response |
| CIS Control 15.1 | Maintain an inventory of authorized wireless access points connected to the wired network. | CMDB |
| CIS Control 16.1 | Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider. | CMDB |
| CIS Control 18.5 | Use only standardized and extensively reviewed encryption algorithms. | Discovery |
| CIS Control 18.8 | Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group. | Vulnerability Response |
| CIS Control 19.1 | Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/ management. | Security Incident Response |
| CIS Control 19.2 | Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution. | Security Incident Response |
| CIS Control 19.3 | Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles. | Security Incident Response |
| CIS Control 19.4 | Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. | Security Incident Response |
| CIS Control 19.6 | Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities. | Security Incident Response |
| CIS Control 19.8 | Create an incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures. | Security Incident Response |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

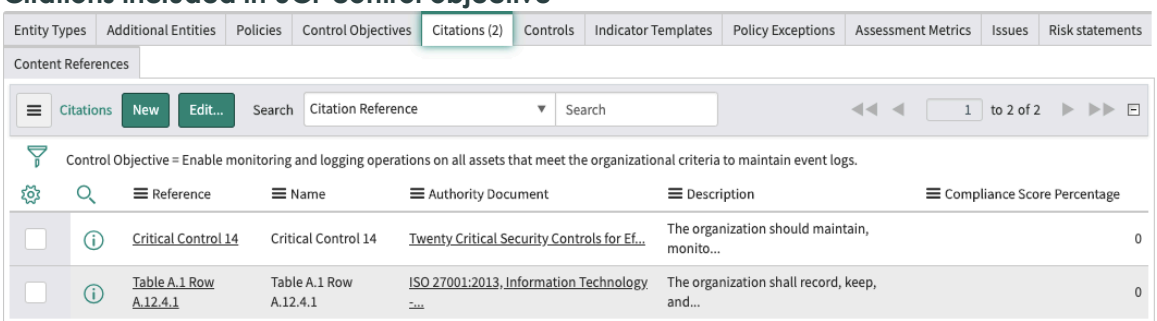
Control objectives that are downloaded from UCF have UCF as the source, as shown below.

**UCF control objective**




If you click the **Citations** related list, you can see that two citations are present: one obtained from CIS and one from ISO 27001 authority documents from UCF.

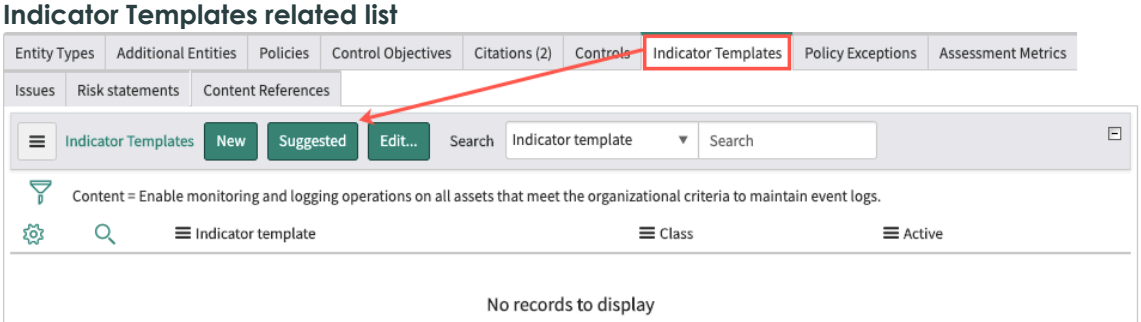
**Citations included in UCF control objective**




These citations allow you to use the CIS controls downloaded from UCF, instead of the CIS Controls included with the Cybersecurity Controls Accelerator application while still associating the controls with the indicator templates provided.

If you want to associate this UCF control objective to similar indicator templates, you can click the **Indicator Templates** related list and then click the **Suggested** button.

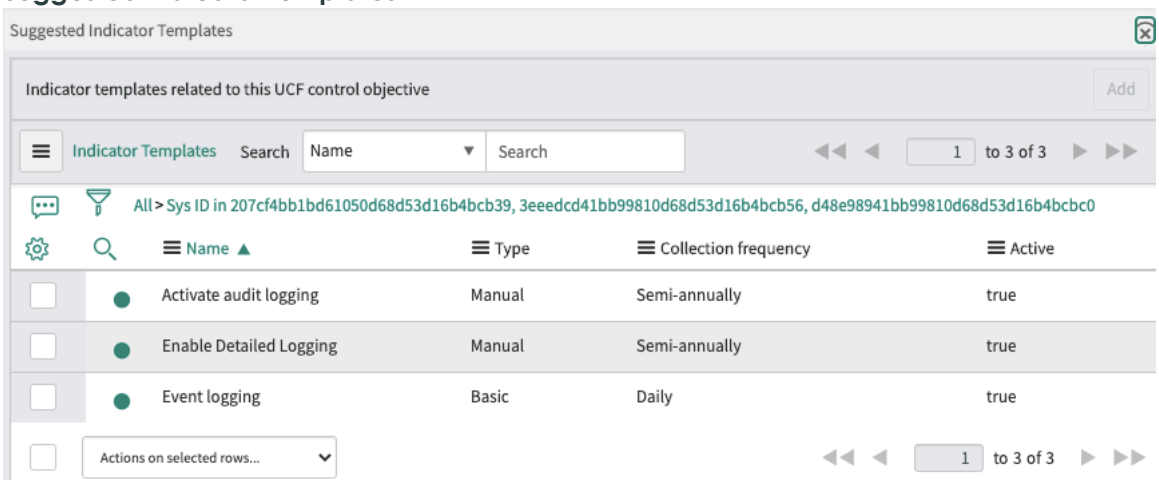
**Indicator Templates related list**




A list of indicator templates that may apply to the selected control objective are shown.

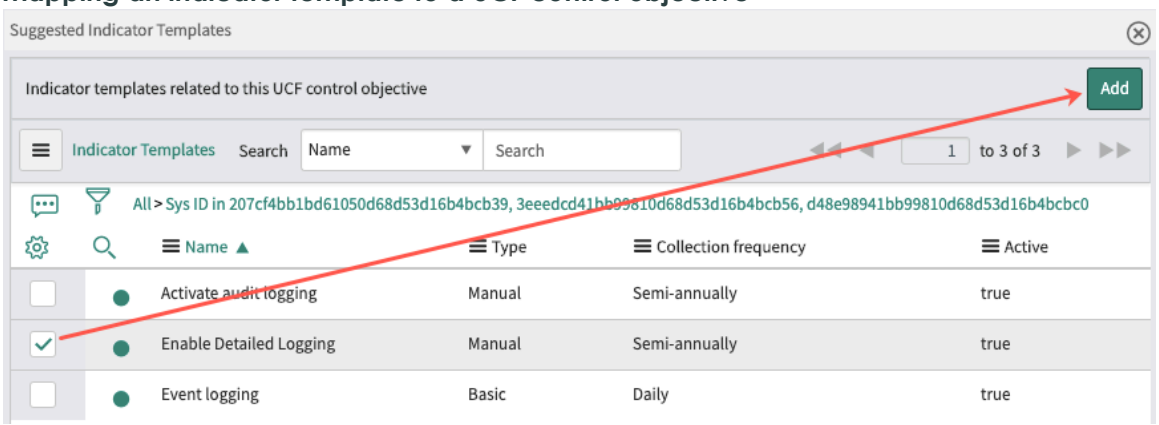
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Suggested indicator templates




Select the indicator templates you want to map to the UCF control objective and click **Add**.

### Mapping an indicator template to a UCF control objective




## GDPR DPIA Use Case Accelerator

The General Data Protection Regulation (GDPR) is a regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU).

**Note:** GRC: GDPR DPIA Accelerator is now deprecated and no longer supported or available for new activation. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

## GDPR DPIA Use Case Accelerator in a nutshell

The ServiceNow® GDPR DPIA Use Case Accelerator allows you to perform data protection impact assessments (DPIA) to protect the personal data of individuals within and outside of the EU. The following diagram and steps describe the flow of the GDPR DPIA Use Case Accelerator system.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

1. A target refers to the association between an entity and a data processing activity. Targets can be created manually or you can generate them automatically by selecting the **Generate target** check box on the entity screen.
2. A preliminary assessment can be performed on a target to determine whether it is deemed to be a high-risk operation and to decide what mitigation procedures are needed.
3. Based on the findings of the preliminary assessment, you can create a DPIA risk to perform a GDPR DPIA assessment. Risk executives and Data Processing Officers can view the progress of the assessment and view responses from individual assessment takers.
4. If an assessment respondent selected mitigation measures in the assessment, a Risk Mitigation task is created after the assessment has been completed.
5. The GDPR DPIA Use Case Accelerator overview dashboard provides an executive view into various data points, such as risks, assessments, and risk mitigation measures, helping the GDPR DPIA GDPR DPIA executives and officers pinpoint areas of concern quickly.

## Assessments performed using the GDPR DPIA Use Case Accelerator

Two types of assessments can be performed: preliminary assessments and GDPR DPIA assessments.

**Preliminary assessments (also known as GDPR DPIA target assessments):** Preliminary assessments are carried out directly on a data processing operation Target. A target contains information that is shared between ServiceNow Governance, Risk, and Compliance applications and use case accelerator applications, including the GDPR DPIA Use Case Accelerator. The target helps evaluate certain key characteristics of the data processing operation, such as its purpose, necessity, and evaluation criteria, and the preliminary assessment helps users arrive at a conclusion and then determine mitigation procedures when the data processing operation is deemed to be a high-risk operation.

**GDPR DPIA assessments:** DPIA assessments are typically performed for high-risk data processing operations; that is, for targets. However, DPIA assessments are not directly evaluated on the targets. They are instead evaluated using the risk assessment functionality provided in the Risk Management application. The DPIA assessments are referred to in the GDPR DPIA Use Case Accelerator context as DPIA Risk.

As an outcome of a preliminary assessment, risk executives can create risks. These are the actual risks that were identified from the evaluation of the target from the preliminary assessment. While it is encouraged risk executives leverage the Risk Management application for recording such risks, they can also record them using the GDPR DPIA Use Case Accelerator application, as described in this section.

**Note:** Two types of content are enabled by the GDPR DPIA Use Case Accelerator application: Core content and Demo content. Core content is directly accessible by the modules you configure in **GDPR DPIA** > **Content**. Demo content is indirectly accessible by the applications in the GRC product suite. Both Core content and Demo content can be viewed using the dashboards and reports.

## Who uses the GDPR DPIA Use Case Accelerator

| Persona | Description |
|---|---|
| Data Protection Officer | Ensures that an organization applies the laws protecting the personal data of individuals. The designation, position, and tasks of a DPO within an organization are described |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Persona | Description |
| --- | --- |
| | in Articles 37, 38, and 39 of the EU General Data Protection Regulation. |
| Risk Executive | Ensures that risks are identified and managed consistently across the organization. Facilitates the data protection impact assessments as per the organization's strategy. |
| Governance, Risk, and Compliance admin | Provides access to all applications under **GDPR** > **Administration**. |

## GDPR DPIA Use Case Accelerator supporting concepts

Familiarize yourself with these concepts, developed from the GDPR DPIA guidance.

| Concept | Description |
| --- | --- |
| Data Processing Operation (or Activity) | Processing covers a wide range of operations performed on personal data. It includes the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of personal data.<br><br>The GDPR applies to the processing of personal data wholly or partly by automated means, as well as to non-automated processing if it is part of a structured filing system.<br><br>A Data Processing Operation (or Activity) in a GDPR DPIA application is a Target (explained below) that is precisely defined for representing a processing operation as described in the GDPR regulation. |
| Data Protection Impact Assessment (DPIA) | A DPIA is an assessment of the impact of data processing operations on the protection of personal data, and more particularly, an assessment of the likelihood and severity of risks for the rights and freedoms of individuals resulting from a processing operation. Under the GDPR, controllers are required to perform DPIA assessments prior to executing a data processing operation that is likely to result in high risk for the rights and freedoms of individuals. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Concept | Description |
| --- | --- |
| | DPIA is a risk assessment in the GDPR DPIA application. The DPIA Register modules facilitate creation, execution, and tracking of the DPIA assessments using the ServiceNow® Risk Management application. A DPIA assessment is initiated in Risk Management and its base system workflow helps drive the DPIA assessment to leverage standard risk assessment features. |
| General Data Protection Regulation (GDPR) | This regulation protects natural persons for the processing of personal data and the free movement of such data. It repeals Directive 95/46/EC (Data Protection Directive).<br>The GDPR DPIA Use Case Accelerator application supports DPIA and provides a structured approach to conducting assessments. |
| High-Risk Processing Operation (or Activity) | This is a processing operation assessed to have a high likelihood and severity of harm and is likely to result in a high risk to the rights and freedoms of natural person. Usually, organizations make a pre-determination (that is, prior to executing a DPIA assessment) if a data processing operation is high-risk based on several factors that are specific to the organization and the nature of their services. DPIAs are usually performed after such a pre-determination.<br>A Data Processing Operation (or Activity) in the GDPR DPIA Use Case Accelerator application is referred to as a Target. A Target can be flagged as "high-risk" to indicate it's a high-risk processing operation. |
| Risk | GDPR outlines various components of the DPIA which overlap with well-defined components of risk management. In risk management terms, a DPIA aims at "managing risks" to the rights and freedoms of natural persons, using the following processes, by:<br>• establishing the context: "taking into account the nature, scope, context and purposes of the processing and the sources of the risk"<br>• assessing the risks: "assess the particular likelihood and severity of the high risk" |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Concept | Description |
| --- | --- |
| | • treating the risks: “mitigating that risk” and “ensuring the protection of personal data”, and “demonstrating compliance with this regulation”<br><br>To facilitate logging of the risks as an outcome of the DPIA assessment, the GDPR DPIA Use Case Accelerator application provides Risk Register and Risk Assessments modules. |
| Target | The target is the foundation of the GDPR DPIA Use Case Accelerator and all related concepts.<br><br>The target is a shared table between the ServiceNow® GRC products and several use case accelerators. They are similar to the concept of entities in the core GRC applications. They are optionally linked to entities, but are used for any attributes that are specific to the use case accelerators. |

### Download the GDPR DPIA Use Case Accelerator

Before you run GRC: GDPR DPIA Use Case Accelerator in your instance, you must download it from the ServiceNow Store. You can then verify the installation.

### Before you begin

**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

Prior to running the GDPR DPIA Use Case Accelerator application, you must download and activate the following GRC applications:

- Audit Management
- Policy and Compliance Management
- Risk Management

Role required: admin

### Procedure

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

### Components installed with GRC: GDPR DPIA Use Case Accelerator

When you have successfully downloaded the GRC: GDPR DPIA Use Case Accelerator, several types of components are installed, including tables, user roles, and scheduled jobs.

Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

**Note:** The Application Files table lists the components that are installed with this application. For instructions on how to access this table, see Find components installed with an application.

Demo data is available for this feature.

### Roles installed

| Role title [name] | Description | Contains roles |
|---|---|---|
| Data Processing Officer<br>[sn_irm_gdpr_dpia.data_processing_officer] | Ensures that an organization applies the laws protecting the personal data of individuals. The designation, position, and tasks of a DPO within an organization are described in Articles 37, 38, and 39 of the EU General Data Protection Regulation. | • sn_risk.manager<br>• sn_irm_gdpr_dpia_user |
| Risk Executive<br>[sn_irm_gdpr_dpia.risk.executive] | Ensures that risks are identified and managed consistently across the organization. Facilitates the data protection impact assessments as per the organization's strategy. | • sn_risk.manager<br>• sn_irm_gdpr_dpia_user |
| GDPR DPIA User<br>[sn_irm_gdpr_dpia.user | Contains the target user role in the sn_grc scope, and the user role in the Risk Management application. | • sn_grc.target_user<br>• sn_risk.user |

## Tables installed

| Table | Description |
|---|---|
| GDPR Preliminary Assessments<br>[sn_irm_gdpr_dpia_m2m_assessment_i_target] | A relationship table that associates preliminary assessments to the GDPR target. |

## Properties Installed

| Name | Description |
|---|---|
| Default DPIA Assessment<br>sn_irm_gdpr_dpia_default_assessment | Compliance administrators can change this setting. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Name | Description |
|---|---|
| | • **Type**: choice list<br>• **Default value**: GDPR DPIA Assessment<br>• **Location**: **GDPR DPIA** > **Administration** > **Properties** |
| GRC Choice - GDPR DPIA Framework<br>sn_irm_gdpr_dpia_default_framework | Compliance administrators can change this setting.<br>• **Type**: choice list<br>• **Default value**: GDPR DPIA<br>• **Location**: **GDPR DPIA** > **Administration** > **Properties** |
| GDPR DPIA Target Assessment<br>sn_irm_gdpr_dpia.gdpr_dpia_targets_assessment | System administrators can change this setting.<br>• **Type**: choice list<br>• **Default value**: GDPR DPIA Targets Assessment<br>• **Location**: **GDPR DPIA** > **Administration** > **Properties** |

### GDPR DPIA Use Case Accelerator module overview

After you have accessed the GDPR DPIA Use Case Accelerator, the application offers many modules.

**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

### GDPR DPIA Use Case Accelerator modules

| Application/ Module | Description |
|---|---|
| **GDPR DPIA** | Application that enables GDPR DPIA Use Case Accelerator application |
| **Overview** | GDPR DPIA executive dashboard |
| **Data Processing Activity** | |
| Create Target | Create a GDPR target. |
| All Targets | List of all target records with a customized view to easily flag them as data processing operation (or activity) |
| My Approvals | List of approvals of Targets awaiting approval of logged user in capacity of a Data Processing Officer (DPO) |
| My Assessments | List of preliminary assessments that can be accessed by logged in user. |
| All Assessments | List of preliminary assessments |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### GDPR DPIA Use Case Accelerator modules (continued)

| Application/ Module | Description |
|---|---|
| **DPIA Register** | |
| New | Module provides ability to create new DPIA Risk |
| In-Progress | List of active DPIA Risks |
| Retired | List of in-active DPIA Risks |
| **DPIA Assessments** | |
| My Assessments | List of GDPR DPIA Assessments that can be accessed by logged in user |
| All Assessments | List of GDPR DPIA Assessments |
| **Risk Register** | |
| New | Module provides ability to create new Risk |
| In-Progress | List of active Risks |
| Retired | List of in-active Risks |
| **Risk Assessments** | |
| My Assessments | List of Risk Assessments that can be accessed by logged in user |
| All Assessments | List of Risk Assessments |
| **DPIA Mitigation Tasks** | |
| My DPIA Mitigation Tasks | List of risk mitigation tasks of DPIA Risks that can be accessed by logged in user |
| All DPIA Mitigation Tasks | List of risk mitigation tasks of DPIA Risks |
| **Content** | |
| Assessment Types | Module provides access to list of all assessments in GDPR DPIA |
| **Administration** | |
| Choices | List of all GRC choices and used to review those configured for GDPR DPIA |
| Properties | Module displays the system properties configured for GDPR DPIA |

### Working with data processing activities

Data Processing Officers can use the options in the Data Processing Activity module to create targets, identify them as data processing activities, and perform GDPR DPIA target assessments on them to determine whether the targets are high risk.

**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Create a target

In the vernacular of the GDPR, a Target refers to the association between an entity and a data processing activity. A GDPR DPIA target assessment is run on a target to identify whether it is a data processing activity, and if the assessment comes back and the target is identified as high-risk, you can create a DPIA risk to run a DPIA assessment on the target to determine how the risk can best be mitigated.

### Before you begin

Role required: sn_irm_gdpr_dpia.risk_executive or sn_irm_gdpr_dpia.data_processing_officer

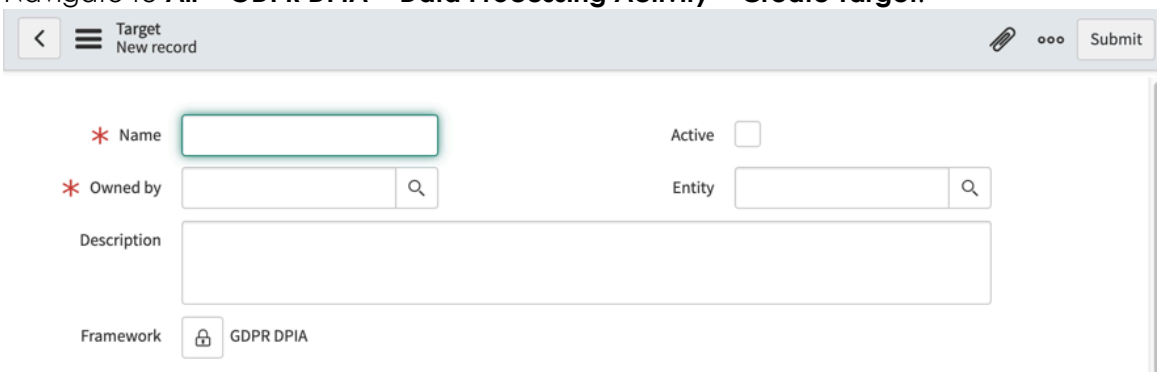
**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

### About this task

Targets can be created manually or you can generate them automatically by selecting the **Generate target** check box on the Entity form or the Entity Type form.

### Procedure

1. Navigate to **All** > **GDPR DPIA** > **Data Processing Activity** > **Create Target**.




2. Fill in the fields, as needed.

| Field | Description |
|---|---|
| Name | Enter the name of the target. |
| Owned by | Select the owner for this target. |
| Description | Enter a description that describes the target. |
| Active | Select this check box to activate the target. |
| Entity | Select the entity associated with this target. An entity can have only one target associated with it. |
| Framework | This field defaults to **GDPR DPIA**. |

3. Do one of the following:
   - To save the data, click **Update**.
   - To identify the target record as a data processing activity, click here.
   - To modify the list of assessment respondents, click the Preliminary Assessments tab.
   - To perform a preliminary assessment on the target, click **Send Assessments**.
   - To perform a DPIA assessment on the target, click **Generate DPIA**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Identify a target as a data processing activity

Identifying a target as a data processing activity is the first step in determining whether a data processing assessment should be performed on the target.

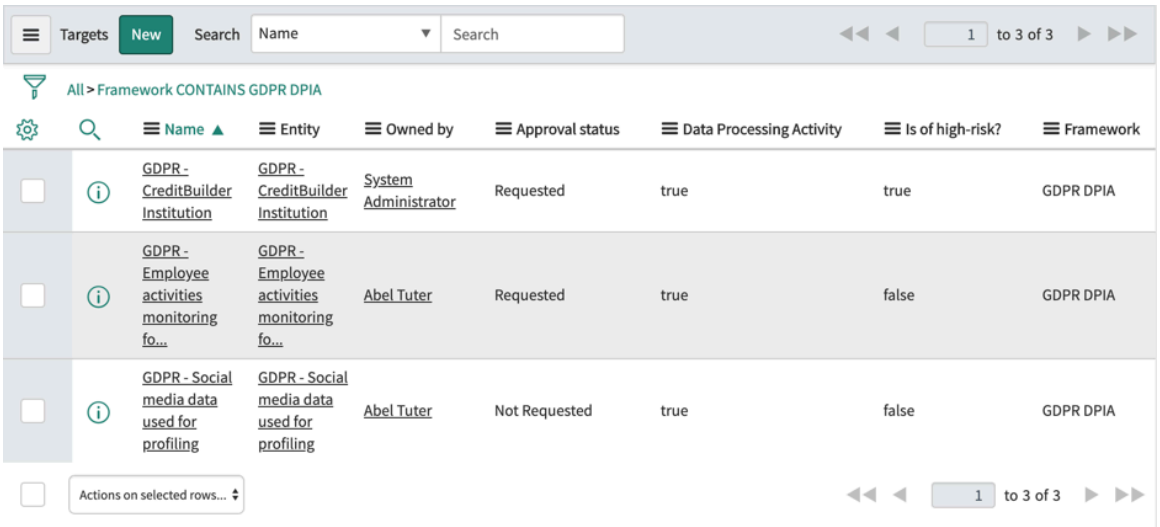
**Before you begin**

Role required: sn_irm_gdpr_dpia.risk_executive or sn_irm_gdpr_dpia.data_processing_officer

**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

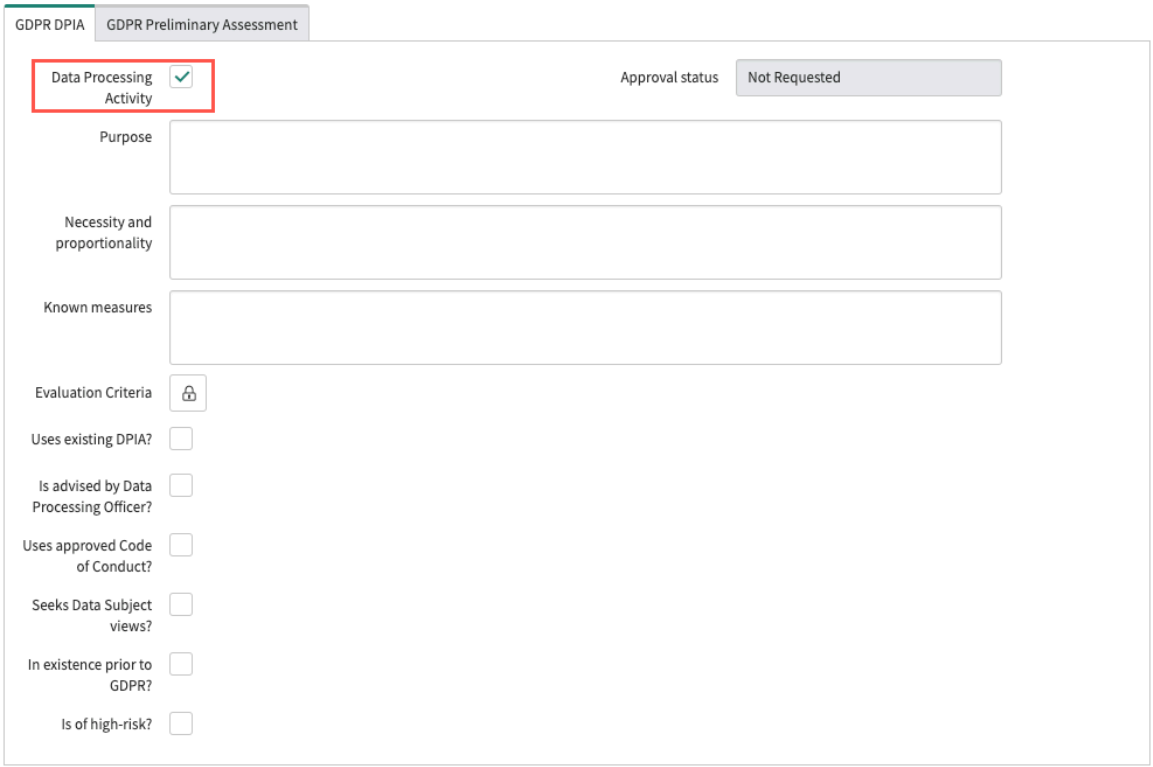
**Procedure**

1. Navigate to **All** > **GDPR DPIA** > **Data Processing Activity** > **All Targets**.




2. Select the target record you want to identify as a data processing activity.
3. Click **Update**.
   Two related lists appear: **GDPR DPIA** and **GDPR Preliminary Assessment**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




4. On the **GDPR DPIA** tab, select the **Data Processing Activity** check box.
5. Fill in the fields, as needed.

| Field | Description |
|---|---|
| Approval Status | Displays the current status of the approval process. |
| Purpose | The purpose of the target. Include information such as where the activity is applicable. |
| Necessity and proportionality | An assessment of the necessity and proportionality of the target in relation to its purpose. |
| Known measures | Measures for addressing the risk, including safeguards, security measures, and mechanisms to ensure the protection or personal data. |
| Evaluation Criteria | Click the lock icon and select the criteria to be considered to evaluate whether the target likely results in high-risk. The criteria are:<br>◦ Evaluation or scoring<br>◦ Automated decision-making with legal or similar significant effect<br>◦ Systematic monitoring<br>◦ Sensitive data or data of a highly personal nature<br>◦ Data processed on a large scale<br>◦ Matching or combining datasets<br>◦ Data concerning vulnerable data subjects |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| | ◦ Innovative use or applying new technological or organizational solutions<br>◦ Preventing data subjects from exercising a right or using a service or contract |
| Uses existing DPIA? | Select this check box if the target uses a pre-existing DPIA, then click the lock icon and select the DPIAs associated with this target from the list. |
| Is advised by Data Processing Officer? | Select this check box if the target requires the approval of a Data Processing Officer, then click the lock icon and select the appropriate Data Processing Officer from the list. |
| Uses approved Code of Conduct? | Select this check box if the target must be compliant with a Code of Conduct when its impact is accessed, then enter the name of the Code of Conduct in the text box. |
| Seeks Data Subject views? | Select this check box if the target requires that the views of data subjects or their representatives be reviewed, then enter the data subject views in the text box. |
| In existence prior to GDPR? | Select this check box if the target existed prior to the creation of the GDPR.<br>**Note:** The requirement to carry out the DPIA applies to all existing data processing activities that are likely to result in a high risk to the rights and freedoms of natural persons for whom there has been a change of the risks. |
| Is of high-risk? | Select this check box this is a high-risk target.<br>**Note:** Even if there are no indications of likely high risk, consider performing a DPIA assessment for any major data processing activities that involve the use of personal data. |

**Note:** You have two options for filling out the fields on the **GDPR DPIA** tab. You can manually fill them out yourself as described above, or if you do not know the answers to the questions, you can generate an assessment for someone else who does, and then copy their responses from the assessment to the target form as describe below.

6. To generate an assessment for another user, perform these steps.

   a. Click the **GDPR Preliminary Assessment** tab.

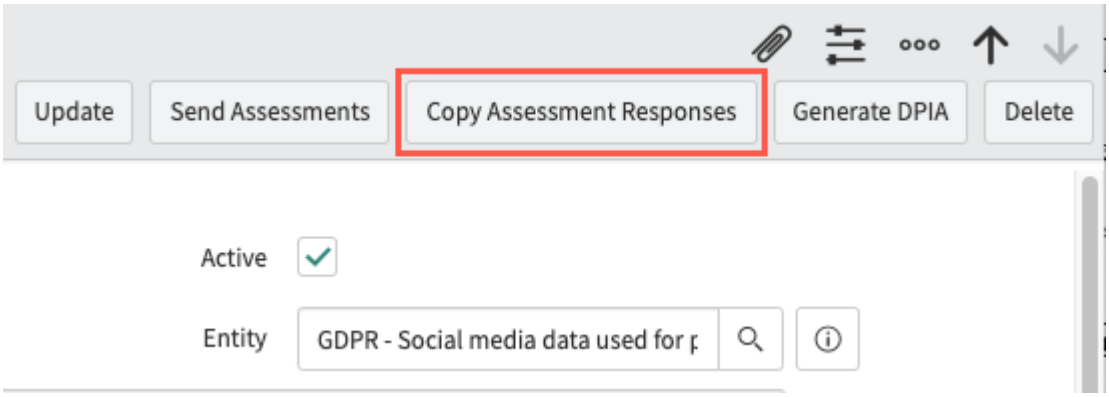
   b. In the **Assessment Respondents** field, click the lock icon and select the user you want to fill out the form.

   c. When you have selected the responder, click the Lock icon again.

   d. Click **Send Assessments**.

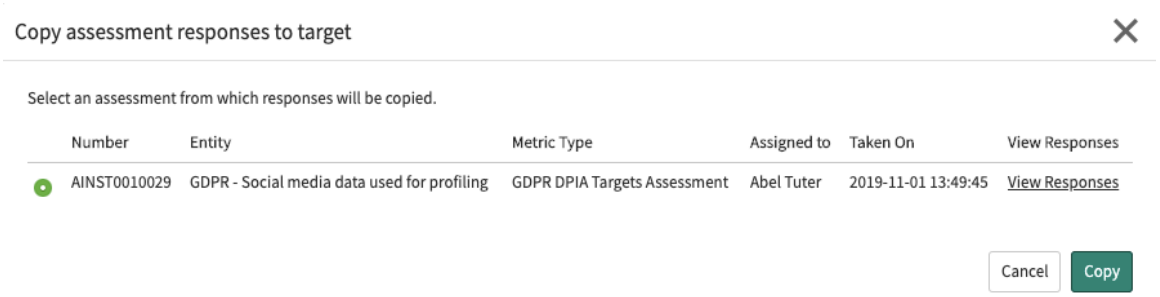
      After the selected user has taken the assessment, a **Copy Assessment Responses** button appears.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**e.** Click **Copy Assessment Responses**.

The completed assessment record is shown.




**f.** You can click **View Response** to view the assessment answers.

**g.** Select the record and click **Copy**.
The answers provided by the selected respondent are copied to the GDPR DPIA.

**7.** When you have completed the fields, do one of the following:

- To save the data, click **Update**.
- To modify the list of assessment respondents, click the **Preliminary Assessments** tab.
- To perform a preliminary assessment on the target, click **Send Assessments**.
- To generate a DPIA risk and initiate a DPIA assessment on the target, click **Generate DPIA**.
- If you selected the **Is advised by Data Processing Officer?** check box and selected an approver, a **Request DPO Approval** button appears. Click this button to request approval from the selected approver. All fields on the GDPR DPIA tab become read-only. If further modification is needed, you can click **Reset Approval**.

### Send a preliminary assessment for a target

You can initiate a preliminary assessment on a target to determine whether it is deemed to be a high-risk operation and to decide what mitigation procedures are needed. After the preliminary assessment is initiated, the selected assessment respondents can take the assessment.

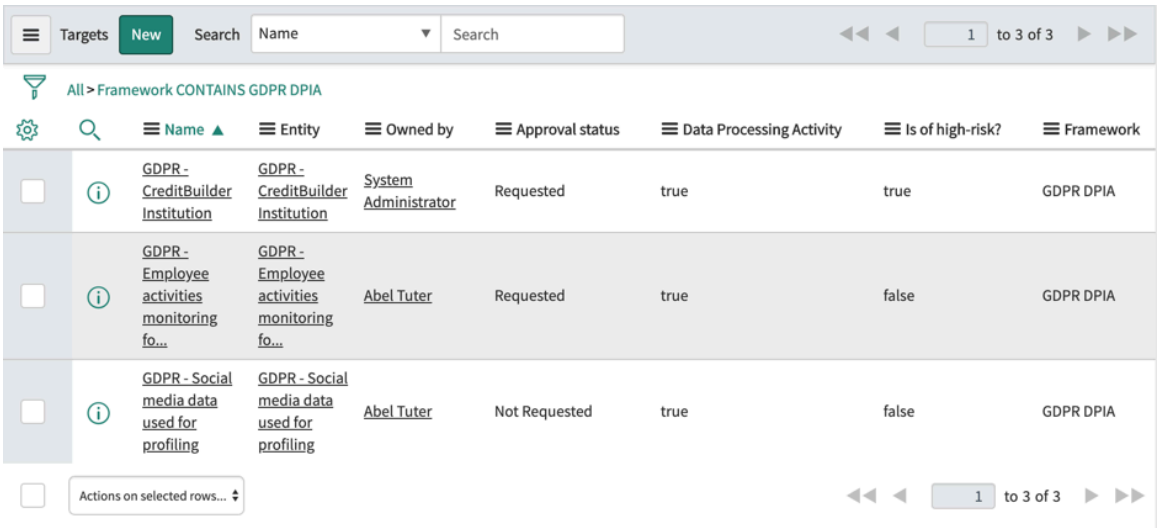
**Before you begin**
Role required: sn_irm_gdpr_dpia.risk_executive or sn_irm_gdpr_dpia.data_processing_officer

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

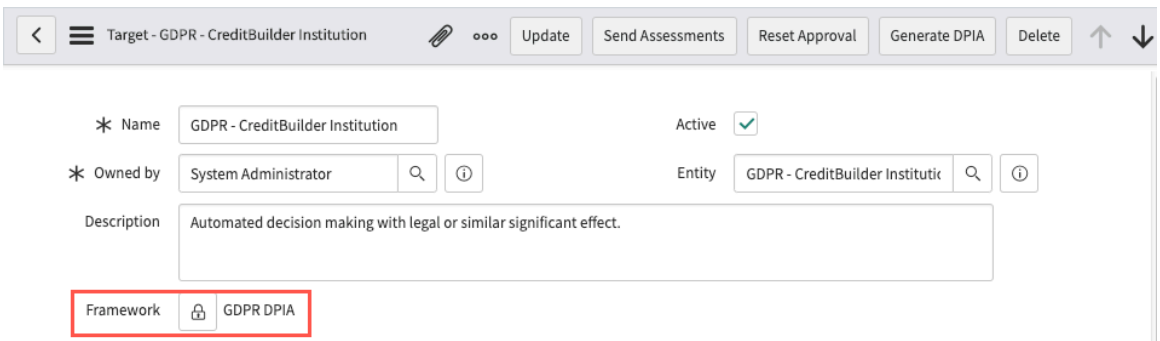
**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

### Procedure

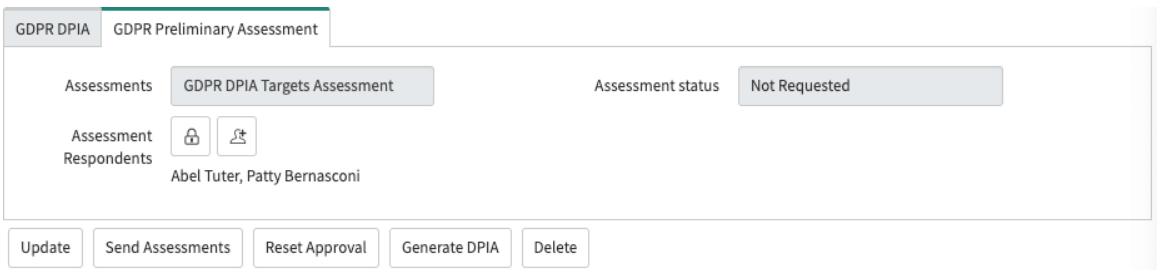
1. Navigate to **All** > **GDPR DPIA** > **Data Processing Activity** > **All Targets**.




2. Open the target record you want to perform a preliminary assessment for.



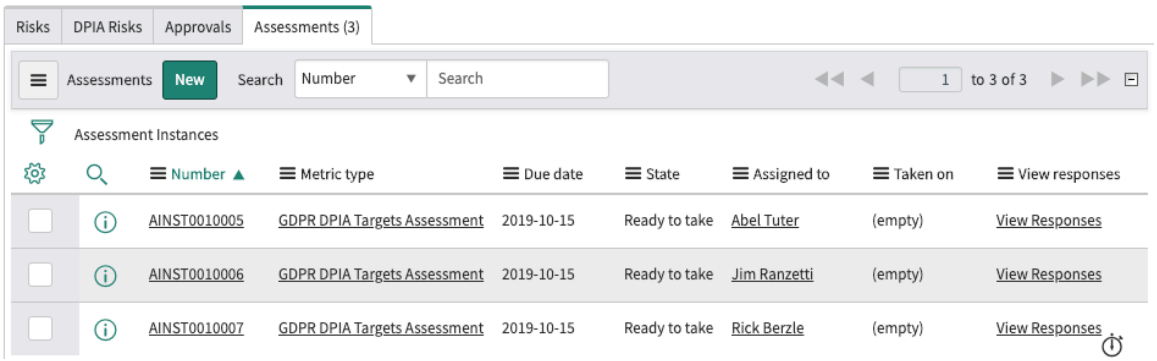

3. Be sure that the **Framework** field shows **GDPR DPIA**.
4. Click the **GDPR Preliminary Assessment** tab.




5. Be sure the **Assessments** field shows **GDPR DPIA Targets Assessment**.
6. In the **Assessment Respondents** field, click the lock icon and select the users you want to take the preliminary assessment for the target.
7. When you have selected the responders, click the Lock icon again.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

8. Click **Send Assessments**.
   The assessments are sent to the selected respondents and a message shows the number of assessments created. Also, the Assessments tab shows the assessment records.




9. To request the Data Processing Officer's approval, click the **Request DPO Approval** related link.
10. After respondents have responded, you can view their responses by clicking **View Responses** on the **Assessments** tab.

### Take a preliminary assessment

When you have been identified as a respondent of a preliminary assessment, you must access and take the assessment.

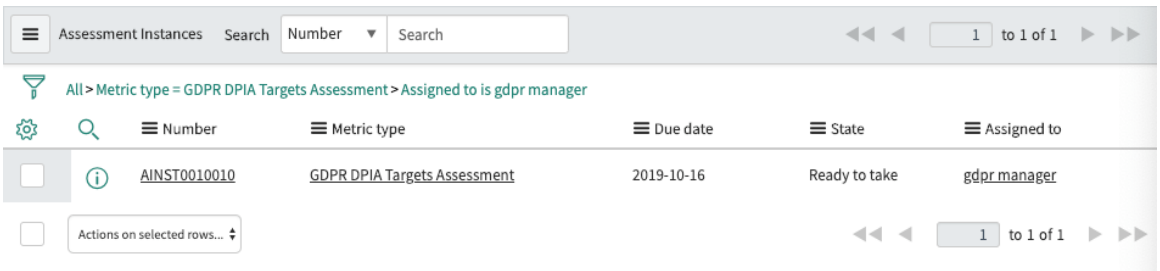
**Before you begin**

Role required: None

**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

**Procedure**

1. Navigate to **All** > **GDPR DPIA** > **Data Processing Activity** > **My Preliminary Assessments**.
   All assessments for which you are a requested respondent are shown.




2. Open the assessment you want to take.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The fields are described here.

| Field | Description |
|---|---|
| Number | Auto-generated record number. |
| Metric type | Metric type of this assessment. |
| Due date | Date by which the assessment must be completed. The system populates the due date from the value in the metric type **Assessment duration** field. The system generates email notifications related to the due date.<br><br>**Note:** By default, the system runs the *Cancel Expired Assessments* script every 30 days to cancel expired survey, assessment, and quiz instances that are in the **Work in progress** or **Ready to take** states. |
| Expiration date | Date by which the assigned user can repeat the assessment. |
| State | State of the assessment. |
| Assigned to | User this assessment is assigned to. This field becomes read-only when the state is **In progress**, **Complete**, or **Canceled**. |
| Signature result | Verification provided by the recipient when a signature is required. This value is either the recipient's full name from the User [sys_user] table or **checked**, indicating that the recipient acknowledged reading the assertion by selecting a check box. |

3. Click **Take Assessment**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




4. Answer the questions to the best of your ability, then click **Submit**.

## View all preliminary assessments

Risk executives and Data Processing Officers can view the responses from individual assessment takers.

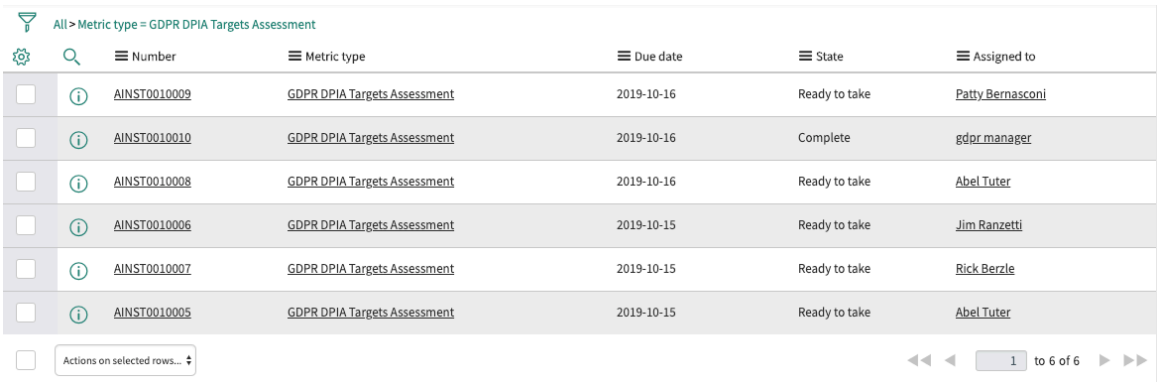
### Before you begin

Role required: sn_irm_gdpr_dpia.risk_executive or sn_irm_gdpr_dpia.data_processing_officer

**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

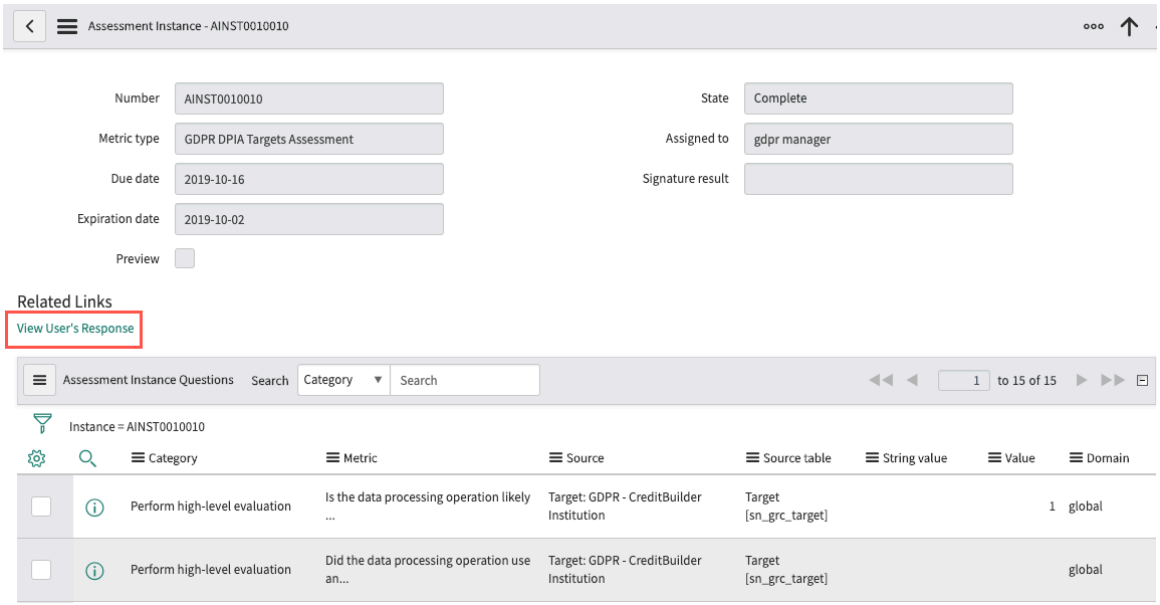
### Procedure

1. Navigate to **All** > **GDPR DPIA** > **Data Processing Activity** > **All Preliminary Assessments**.




2. Click the assessment number of the assessment you want to review.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




3. Click the **View User's Response** related link.

### Working with DPIA risk assessments

After a preliminary assessment has been used to determine that a target posed a high risk, Risk Executives and Data Processing Officers can use the options in the DPIA Register module to create, execute, and track DPIA risk assessments. Depending on whether mitigation measures were selected on a GDPR DPIA assessment, a risk mitigation task is created from the selected list of mitigation measures in the completed assessment.

**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

### Create a new risk record and initiate a DPIA assessment

Using the options in the DPIA Register module, you can create risk records and track their life cycle. DPIA assessments are initiated on risk records.

**Before you begin**

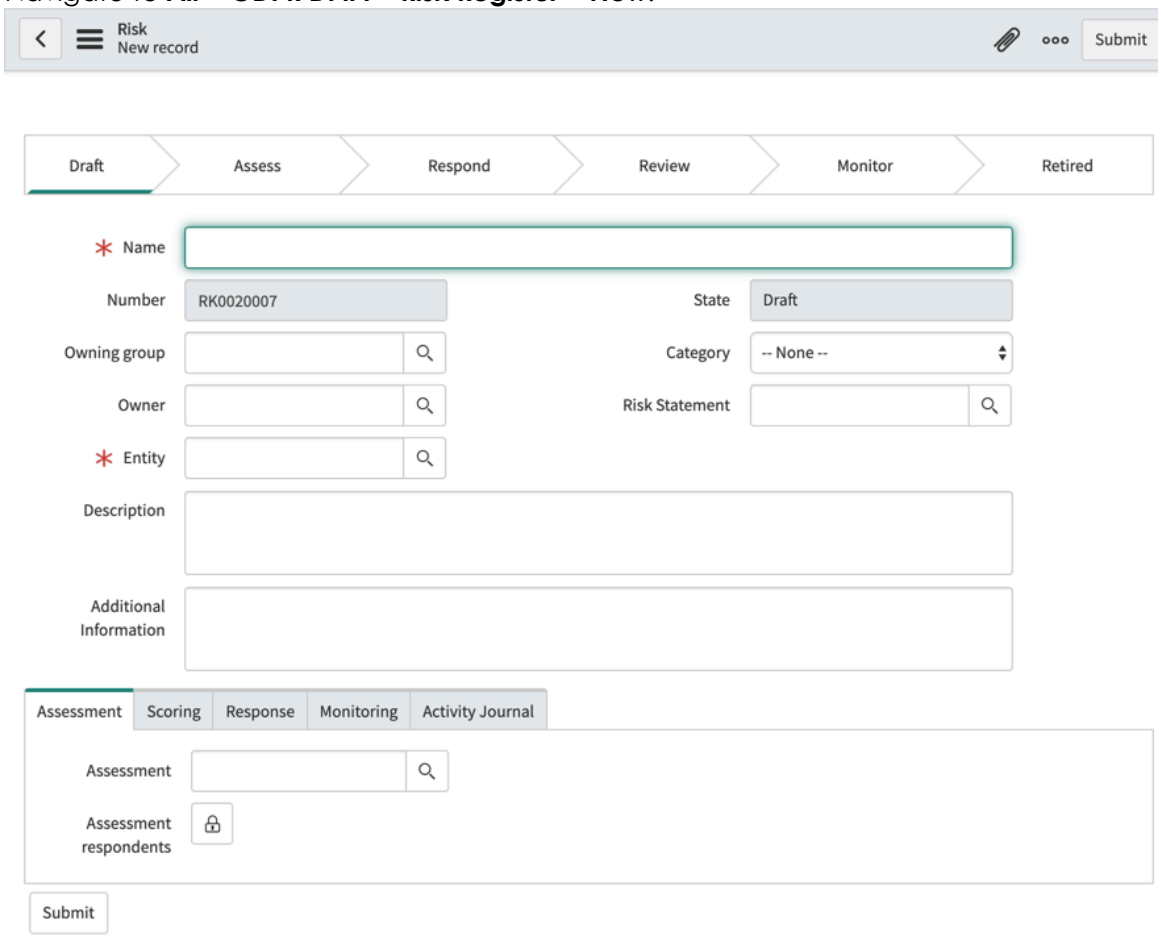
Role required: sn_irm_gdpr_dpia.risk_executive or sn_irm_gdpr_dpia.data_processing_officer

**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

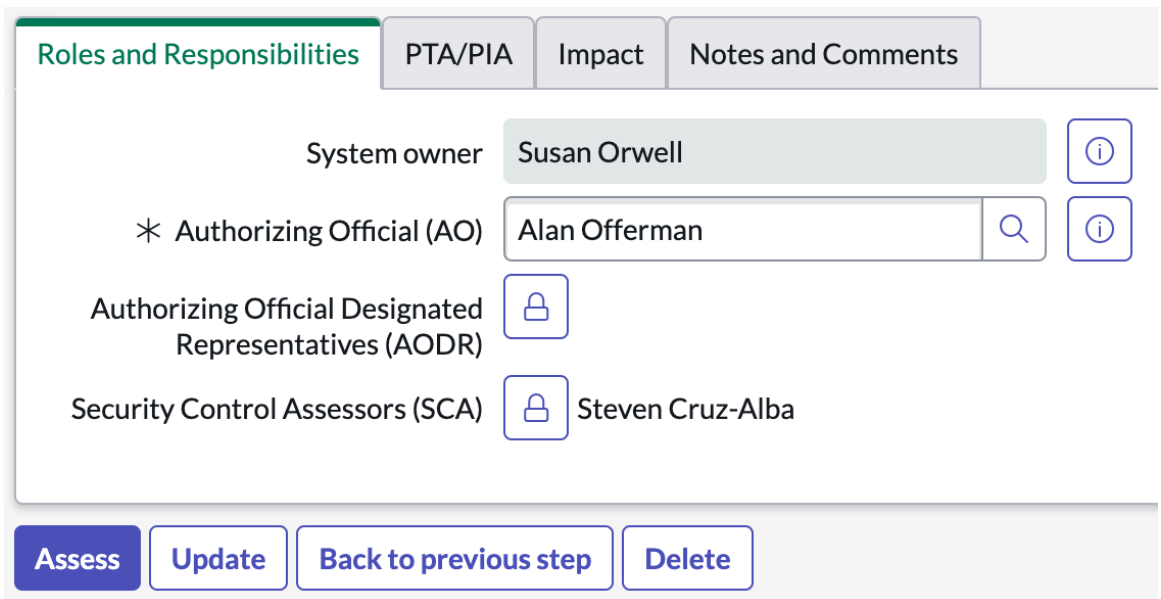
## Procedure

1. Navigate to **All** > **GDPR DPIA** > **Risk Register** > **New**.




2. Fill in the fields, as described here.
3. When you have completed your entries, save the record.

   An **Assess** button appears.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To initiate the assessment, click **Assess**.
   The risk record transitions to the Assess state and a message shows the number of assessments that were sent.

Related topics

View assessment responses for an individual respondent

### Take a DPIA assessment

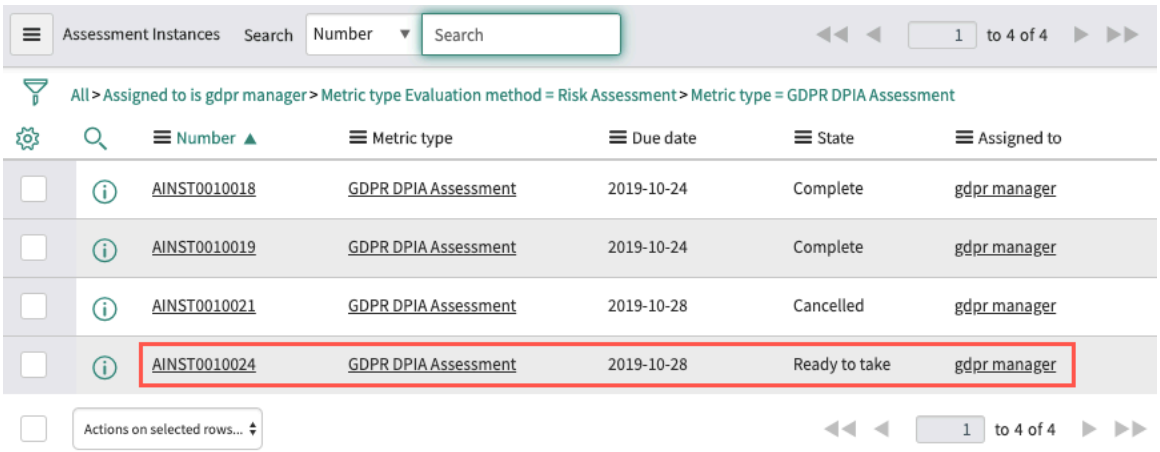
When you have been identified as a respondent of a DPIA assessment, you must access and take the assessment.

**Before you begin**
Role required: None

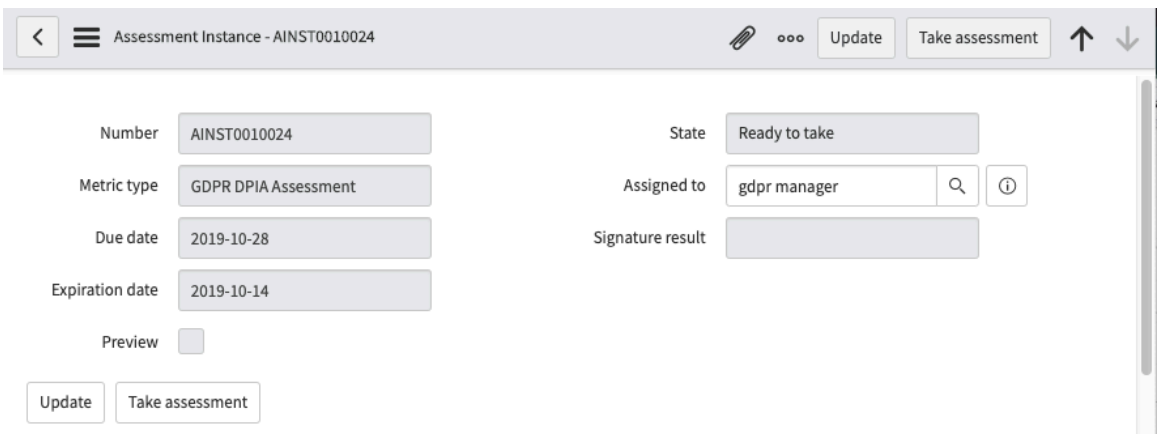
**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

**Procedure**

1. Navigate to **All** > **GDPR DPIA** > **DPIA Assessments** > **My Assessments**.
   All DPIA risk assessments for which you are a requested respondent are shown.




2. Open the assessment you want to take.

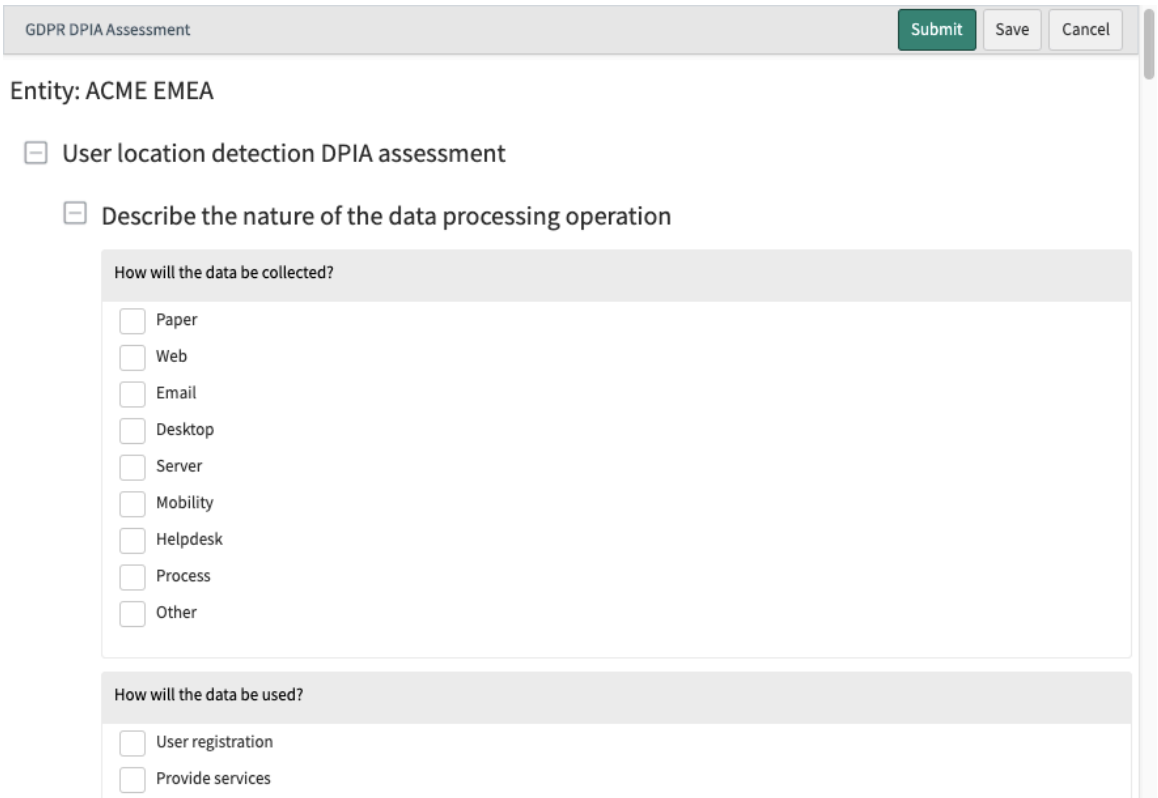



The fields are described here.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Number | Auto-generated record number. |
| Metric type | Metric type of this assessment. |
| Due date | Date by which the assessment must be completed. The system populates the due date from the value in the metric type **Assessment duration** field. The system generates email notifications related to the due date.<br><br>**Note:** By default, the system runs the *Cancel Expired Assessments* script every 30 days to cancel expired survey, assessment, and quiz instances that are in the **Work in progress** or **Ready to take** states. |
| Expiration date | Date by which the assigned user can repeat the assessment. |
| State | State of the assessment. |
| Assigned to | User this assessment is assigned to. This field becomes read-only when the state is **In progress**, **Complete**, or **Canceled**. |
| Signature result | Verification provided by the recipient when a signature is required. This value is either the recipient's full name from the User [sys_user] table or **checked**, indicating that the recipient acknowledged reading the assertion by selecting a check box. |

3. Click **Take Assessment**.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Answer the questions to the best of your ability, then click **Submit**.

> **Note:** The last question in the assessment allows you select one or more mitigation measures. If you selected one or more measures, a Risk Mitigation task is automatically created, and the **Response** field on the risk is set to **Mitigate**.

### View the progress of responses for an assessment

Risk executives and Data Processing Officers can view the responses from all assessment takers while the assessment is in progress. The percentage completed for each respondent is shown.

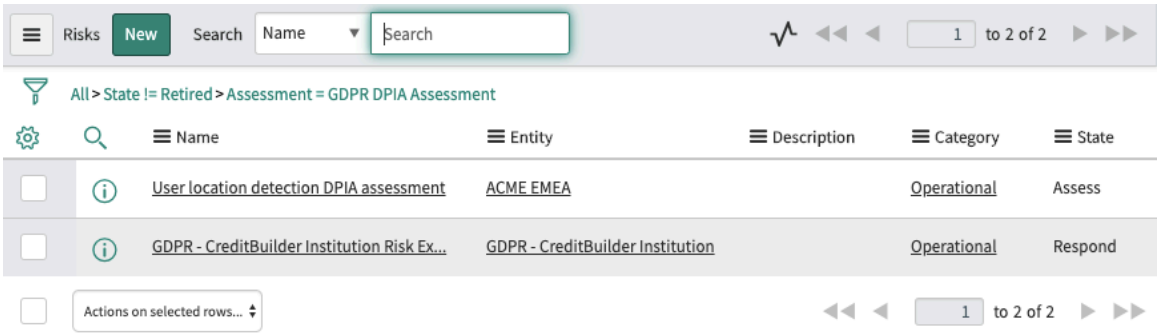
#### Before you begin

Role required: sn_irm_gdpr_dpia.risk_executive or sn_irm_gdpr_dpia.data_processing_officer

> **Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

#### Procedure

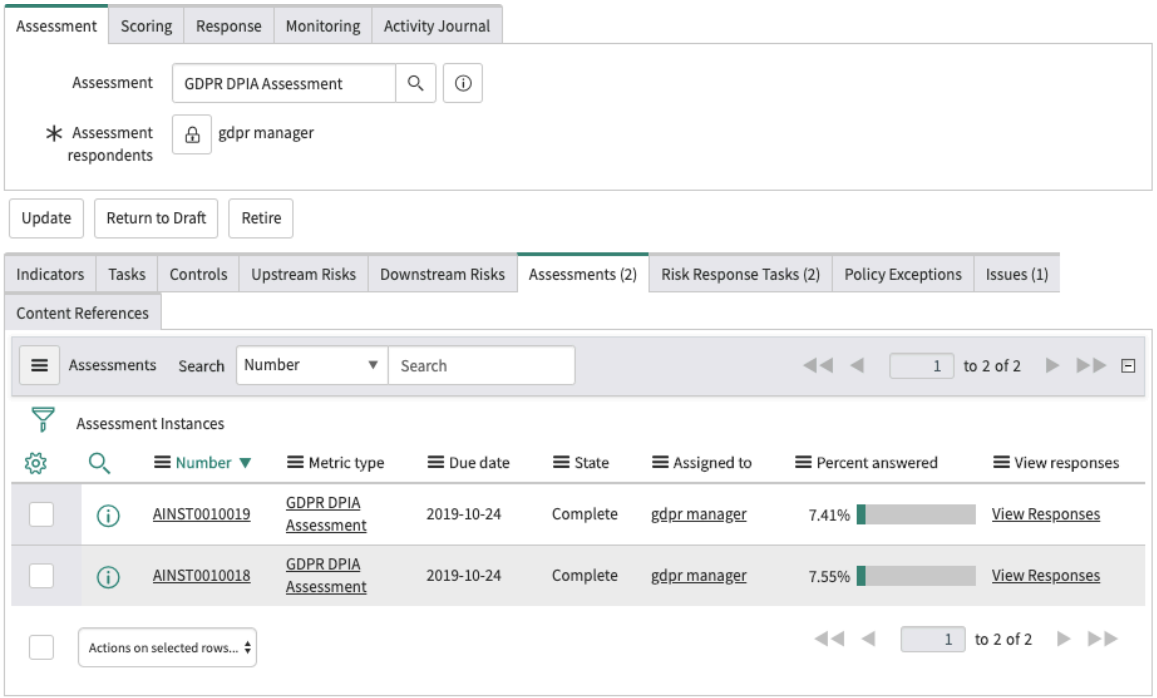
1. Navigate to **All** > **GDPR DPIA** > **DPIA Register** > **In-Progress**.




2. Click the assessment for which you want to view the progress of respondents, then scroll down to the **Assessments** tab.

> **Note:** The assessment must be in the **Respond** state.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**3.** To view the completed responses for an individual respondent, click **View Responses**.

### View assessment responses for an individual respondent

Risk executives and Data Processing Officers can view the responses from individual assessment takers.

### Before you begin

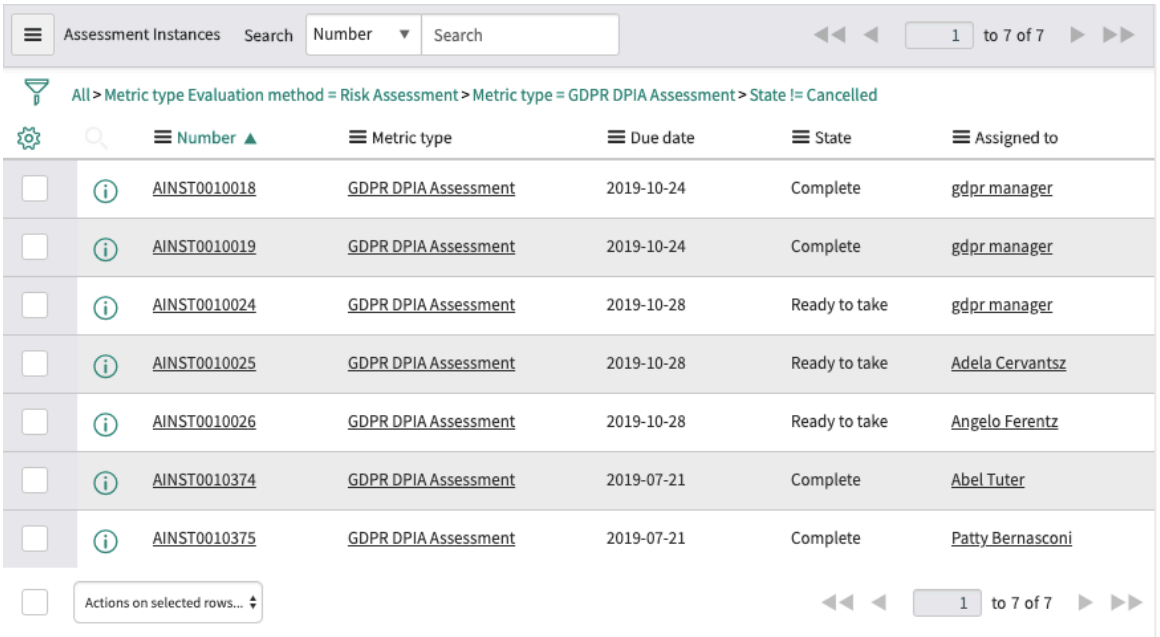
Role required: sn_irm_gdpr_dpia.risk_executive or sn_irm_gdpr_dpia.data_processing_officer

**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

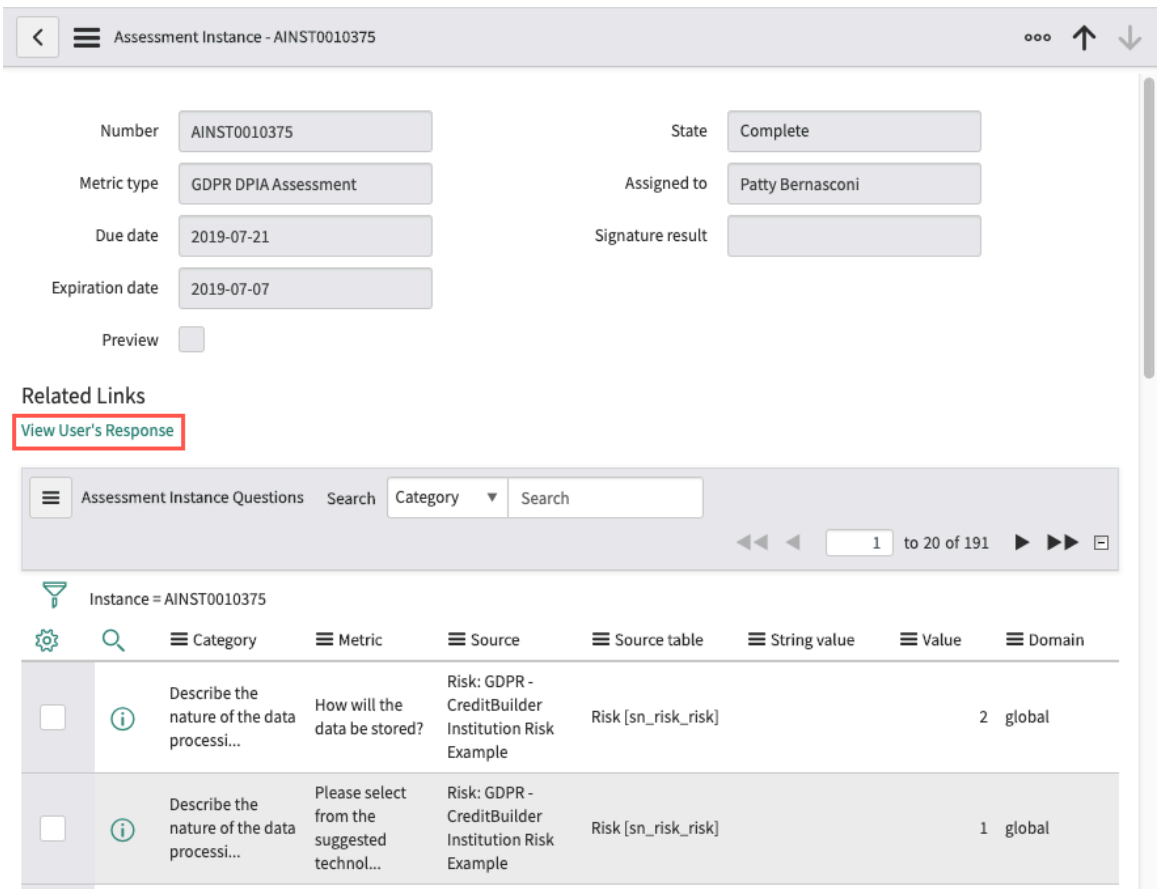
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

**1.** Navigate to **All** > **GDPR DPIA** > **DPIA Assessments** > **All Assessments**.

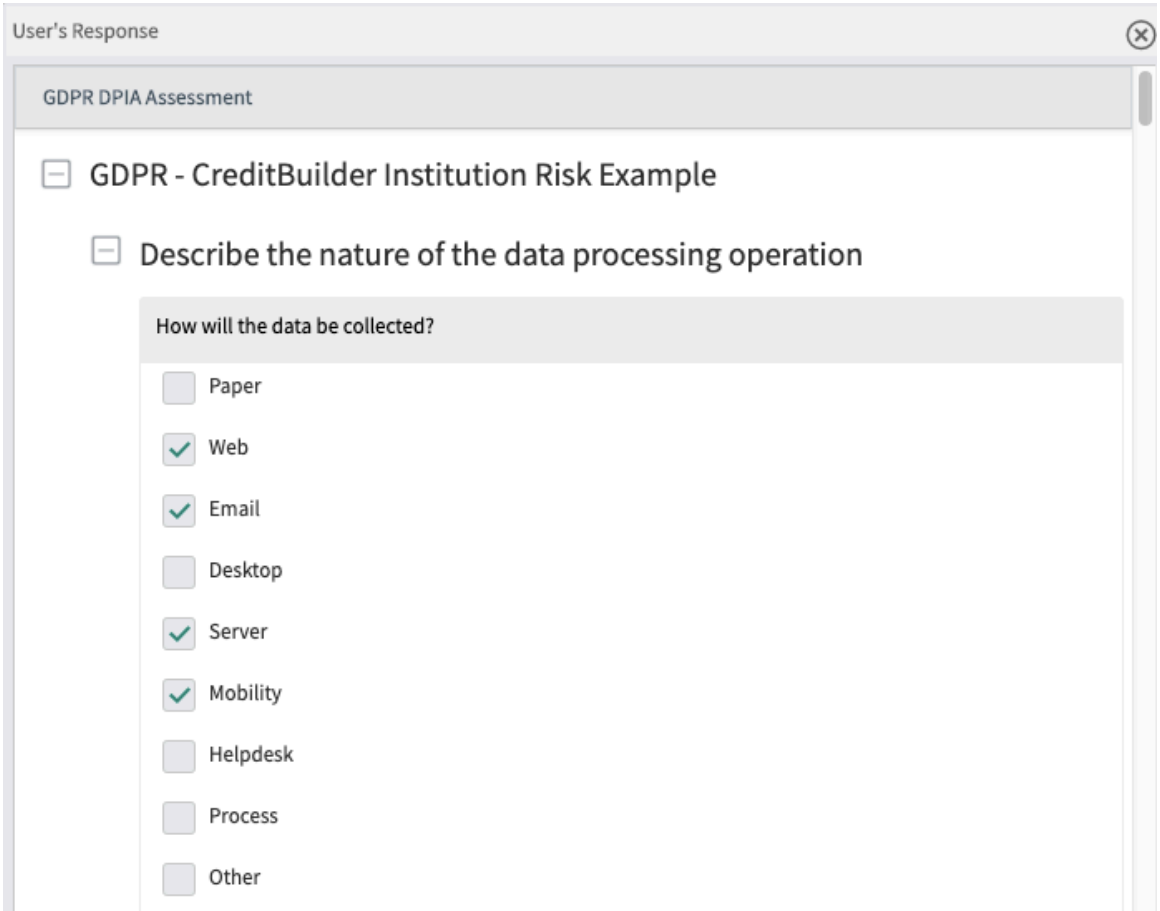



**2.** Click the assessment number of the assessment you want to review.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click the **View User's Response** related link.



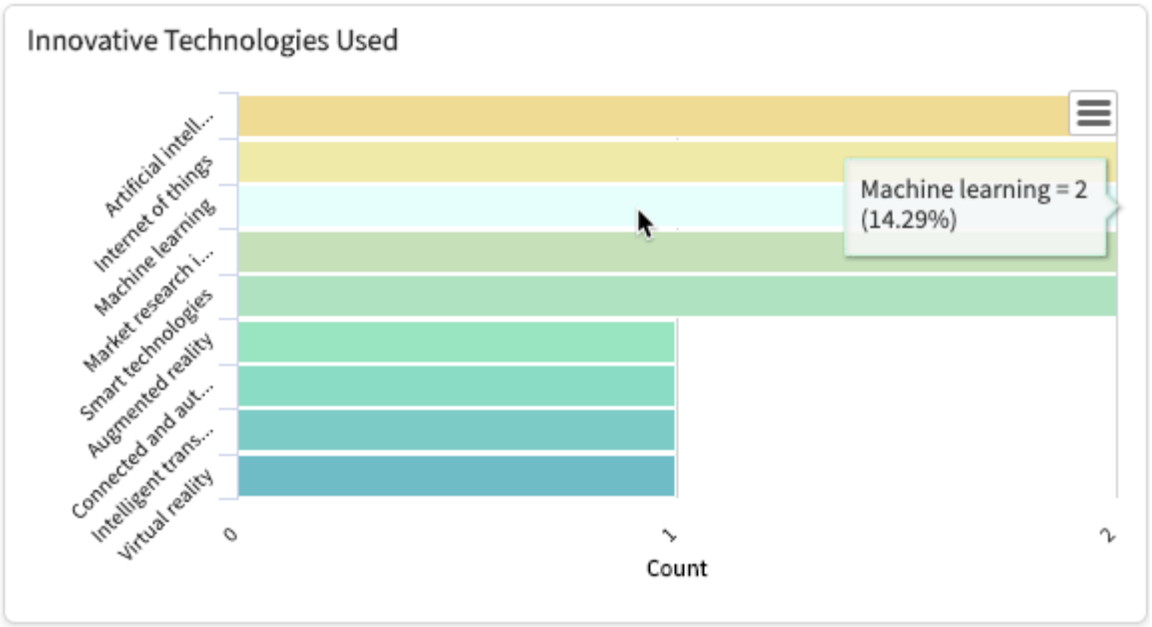

### Working with GDPR DPIA overview dashboards and reports

The GDPR DPIA Use Case Accelerator overview dashboard provides an executive view into various data points, such as risks, assessments, and risk mitigation measures, helping the GDPR DPIA executives and officers pinpoint areas of concern quickly.

**Note:** Starting with the Rome release, GRC: GDPR DPIA Accelerator is being prepared for future deprecation. It will be hidden and no longer activated on new instances, but will continue to be supported. For details, see the Deprecation Process [KB0867184] article in the Now Support knowledge base.

To view the reports, navigate to **GDPR DPIA** > **Overview**. In each chart, you can point to any part of a chart (bar, pie, data point, and so on) to view general data specific to that part. If you click any part of a report, a list opens to provide detailed information.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




## Note:

If customized dashboards are needed, see Create and use dashboards for more information.

### Reports on the Activity Overview tab

| Name | Visual | Description |
|---|---|---|
| High Risk | Single Score | Metric indicates count of data processing operations identified as high risk. |
| Missing DPO Review | Single Score | Metric indicates count of data processing operations not reviewed by Data Processing Officer (DPO). |
| Missing Code of Conduct | Single Score | Metric indicates count of data processing operations not leveraging approved code of conduct. |
| Missing Data Subject Views | Single Score | Metric indicates count of data processing operations not seeking data subject views. |
| Preexisting GDPR | Single Score | Metric indicates count of data processing operations existing before GDPR regulation came into effect. |
| Using Existing DPIA | Single Score | Metric indicates count of data processing operations using existing DPIA assessment. |
| Assessment Status | Horizontal bar | Review data processing operations by preliminary assessment status. |
| Approval Status | Horizontal bar | Review data processing operations by approval status. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Reports on the Nature tab

| Name | Visual | Description |
|---|---|---|
| Data Collection Methods | Horizontal bar | Review assessment responses for data processing operations by collection methods. |
| Data Collection Sources | Horizontal bar | Review assessment responses for data processing operations by collection sources. |
| Data Storage Methods | Horizontal bar | Review assessment responses for data processing operations by storage methods. |
| Data Deletion Methods | Horizontal bar | Review assessment responses for data processing operations by deletion methods. |
| Data Usage | Horizontal bar | Review assessment responses for data processing operations by usage. |
| Data Retention Period | Horizontal bar | Review assessment responses for data processing operations by retention periods. |
| Security Measures | Horizontal bar | Review assessment responses for data processing operations by security concern measures. |
| Innovative Technologies Used | Horizontal bar | Review assessment responses for data processing operations by innovative technologies used. |

### Reports on the Scope tab

| Name | Visual | Description |
|---|---|---|
| Data Collection Size | Horizontal bar | Review assessment responses for data processing operations by data collection sizes. |
| Data Collection Frequency | Horizontal bar | Review assessment responses for data processing operations by collection frequency. |
| Data Sensitivity | Horizontal bar | Review assessment responses for data processing operations by data sensitivity. |
| Individuals Affected | Horizontal bar | Review assessment responses for data processing operations by individuals affected. |
| Geographic Areas Covered | Horizontal bar | Review assessment responses for data processing operations by geographic areas. |

### Reports on the Context tab

| Name | Visual | Description |
|---|---|---|
| Nature of Relationships | Horizontal bar | Review assessment responses for data processing operations by relationships with individuals. |
| Level of Control Offered | Horizontal bar | Review assessment responses for data processing operations by control offered to individuals. |
| Data Processing Concerns | Horizontal bar | Review assessment responses for data processing operations by processing concerns. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Reports on the Context tab (continued)

| Name | Visual | Description |
|---|---|---|
| Current State of Technology | Horizontal bar | Review assessment responses for data processing operations by the current state of technology. |
| Issues of Public Concern | Horizontal bar | Review assessment responses for data processing operations by issues of public concern. |

### Reports on the Consent tab

| Name | Visual | Description |
|---|---|---|
| Consent Methods | Horizontal bar | Review assessment responses for data processing operations by consent methods. |

### Reports on the Assess tab

| Name | Visual | Description |
|---|---|---|
| Lawful Basis for Processing | Horizontal bar | Review assessment responses for data processing operations by lawful basis for processing. |
| International Transfer Safeguards | Horizontal bar | Review assessment responses for data processing operations by international transfer safeguards. |
| Data Quality and Data Minimization Measures | Horizontal bar | Review assessment responses for data processing operations by data quality and data minimization. |
| Processor Compliance Measures | Horizontal bar | Review assessment responses for data processing operations by measures processors take to comply. |
| Individual Rights Measures | Horizontal bar | Review assessment responses for data processing operations by measures to support user rights. |

### Reports on the Mitigate tab

| Name | Visual | Description |
|---|---|---|
| Likelihood of Harm | Heatmap | Review assessment responses for data processing operations by likelihood of harm. |
| Severity of Harm | Heatmap | Review assessment responses for data processing operations by severity of harm. |
| DPIA Open Issues | Horizontal bar | Review DPIA open issues for data processing operations by priority and state. |
| DPIA Open Response Tasks | Horizontal bar | Review DPIA-related response tasks for data processing operations by priority and state. |
| Suggested Mitigation Measures | Horizontal bar | Review assessment responses for data processing operations by mitigation measures. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## NIST CSF Use Case Accelerator

The NIST CSF Use Case Accelerator gives customers an operational head-start when adopting the NIST CSF. When the accelerator is downloaded and activated in the GRC applications, pre-configured policies, scopes (profiles, profile type recommendations), indicators, risks, and other GRC elements appear.

## Who uses the NIST CSF Use Case Accelerator

| Persona | Description |
|---|---|
| Risk executive | Ensures that risks are identified and managed consistently across the organization.<br><br>Defined access to the following sections:<br>• **NIST CSF** > **Overview**<br>• **NIST CSF** > **Framework Core**<br>• **NIST CSF** > **Framework Profiling**<br>• **NIST CSF** > **Content** |
| Security officer | Addresses gaps, non-compliant controls, risks, issues, failed indicators, and action plans for the organizations cybersecurity.<br><br>Defined access to the following sections:<br>• **NIST CSF** > **Framework Core**<br>• **NIST CSF** > **Framework Profiling** |
| Control provider | Helps build a library of cybersecurity controls for the organization.<br><br>Defined access to the following sections:<br>• **NIST CSF** > **Framework Core**<br>• **NIST CSF** > **Content** |
| Sys admin | Access to the following sections: **NIST CSF** > **Administration** |
| GRC admin | Access to the following sections: **NIST CSF** > **Administration** |

### Install the NIST CSF Use Case Accelerator

The NIST Cybersecurity Framework (CSF) Use Case Accelerator is used with the GRC core applications: Policy and Compliance Management, Risk Management, and Audit Management applications.

**Before you begin**
Role required: none.

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Setup task | Description |
| --- | --- |
| Verify that the following applications have been installed:<br>• Policy and Compliance Management<br>• Risk Management<br>• Audit Management | To verify that these applications are activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased. |
| Verify that you have the required roles. | The System Admin (admin) assigns the following roles:<br>• Policy and Compliance Management roles<br>◦ Attestation Creator (sn_compliance.attestation_creator)<br>◦ Compliance Administrator (sn_compliance.admin)<br>◦ Compliance Developer (sn_compliance.developer)<br>◦ Compliance Manager (sn_compliance.manager)<br>◦ Compliance Reader (sn_compliance.reader)<br>◦ Compliance User (sn_compliance.user)<br>• Risk Management roles<br>◦ Risk Admin (sn.risk.admin)<br>◦ Risk Reader (sn.risk.reader)<br>◦ Risk Manager (sn.risk.manager)<br>◦ Risk User (sn.risk.reader)<br>• Audit Management roles<br>◦ Audit Admin (sn_audit.admin)<br>◦ Audit Developer (sn_audit.developer)<br>◦ Audit Manager (sn_audit.manager)<br>◦ Audit User (sn_audit.user)<br>◦ External Auditor (sn_audit.external_auditor) |

### Procedure

1. Log in to the instance you want to install the application on.
2. Navigate to **System Applications** > **All Available Applications** > **All**.
3. Locate the **GRC: NIST CSF Accelerator** application.
4. If you want to load demo data, select the **Demo Data** check box.
5. Click **Install**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Verify the NIST CSF Use Case Accelerator

After installing the GRC: NIST Cybersecurity Framework (CSF) Use Case Accelerator, review the NIST CSF application structure, core content, and demo data, if selected during installation.

**Before you begin**
Role required: admin

**Procedure**

1. Navigate to **All** > **User Administration** > **Roles** and review the roles installed with the NIST CSF application.

   These roles contain nist_csf in their names; for example, sn_irm_nist_csf.security_officer. The roles are associated with NIST CSF application modules to provide access based on the user's role.

   **Note:** The basic NIST CSF user role is needed to access the application. This role contains the reader or user roles from the ServiceNow® GRC suite of applications.

2. In the Application Navigator, type **NIST CSF**, and verify the application core content.

| Navigate to | Verify |
|---|---|
| **NIST CSF** > **Content** > **Policy Statements** | Review the Policies and Policy Statements installed for NIST CSF. |
| **NIST CSF** > **Content** > **Risk Statements** | Review the Risk Frameworks and Risk Statements installed for NIST CSF. |
| **NIST CSF** > **Content** > **Test Templates** | Review the Test Templates installed for NIST CSF. |
| **NIST CSF** > **Content** > **Indicator Templates** | Review the Indicator Templates installed for NIST CSF. |
| **NIST CSF** > **Content** > **Attestation Types** | Review the Control Attestation Types installed for NIST CSF. |
| **NIST CSF** > **Content** > **Assessment Types** | Review the Risk Assessment Types installed for NIST CSF. |

3. Validate the application demo content, if loaded.

| Navigate to | Verify |
|---|---|
| **NIST CSF** > **Orient Targets** | Review the sample Targets installed in the system for use with the NIST CSF application. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Navigate to | Verify |
|---|---|
| **User Administration** > **Users** | Review the sample Persona users installed in the system for use with the NIST CSF application. The User IDs for these users end with .CSF and their name contains CSF. |
| **Policy and Compliance** > **Scoping** > **Profile Classes** | Perform a search for profile classes with the **Name** field containing **with NIST**. Review their relationships by reviewing their roll up to field in respective profile classes. |
| **Policy and Compliance** > **Scoping** > **entity types** | Perform a search for entity types with the **Name** field starting with **NIST CSF**. |
| **Policy and Compliance** > **Policies and Procedures** > **All Controls** | Perform a search for all controls referencing **Control Objectives** with a **Source = NIST CSF**. |
| **Risk** > **Risk Register** > **All Risks** | Perform a search for all risks referencing **Risk Statements** with a **Source = NIST CSF**. |
| **Audit** > **Audit Testing** > **Test Plans** | Perform a search for test plans with **Test Templates** that begin with **NIST CSF**. |
| **Policy and Compliance** > **Indicators** > **Indicators** | Perform a search for all indicators where **Item.Content.Source = NIST CSF**. |
| **Risk** > **Indicators** > **Indicators** | Perform a search for all indicators where **Item.Content.Source = NIST CSF**. |
| **Policy and Compliance** > **Issues** > **All Issues** | Perform a search for all issues where**Item.Content.Source = NIST CSF**. |
| **Risk** > **Issues** > **All Issues** | Perform a search for all issues where **Item.Content.Source = NIST CSF**. |
| **Policy and Compliance** > **Remediation Tasks** > **All Open Remediation Tasks** | Perform a search for all Remediation tasks where an issue identified on the remediation task has**Item.Content.Source = NIST CSF**. |
| **Risk** > **Remediation Tasks** > **All Open Remediation Tasks** | Perform a search for all Remediation tasks where an issue identified on the remediation task has **Item.Content.Source = NIST CSF**. |

### NIST CSF supporting concepts

Familiarize yourself with these concepts, developed from the NIST CSF guidance.

| Concept | Description |
|---|---|
| Target | The target is the foundation of the NIST Cybersecurity Framework (CSF) Use Case Accelerator and all related concepts.<br><br>The target is a shared table between the ServiceNow® GRC products and several Use Case Accelerators. They are similar to |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Concept | Description |
| --- | --- |
| | the concept of entities in the core GRC applications. They are optionally linked to profiles, but are used for any attributes that are specific to the Use Case Accelerators. |
| Critical infrastructure (or critical in NIST CSF application usage) | Vital physical or virtual systems and assets that have a serious impact on cybersecurity, national economic security, and national public health or safety. |
| Implementation tiers | Helps an organization view cybersecurity risks and the processes they use to manage those risks.<br><br>Tiers are prioritized for achieving cybereecurity objectives. With the NIST CSF applications, organizations can evaluate targets from the implementation tier view, which uses the Tier attribute on Target table. |
| Cybersecurity activity | Cybersecurity policies and requirements are found in the ServiceNow® GRC Policy and Compliance Management application. The application provides guidelines for understanding cybersecurity outcomes that need to be achieved to strengthen cybersecurity practices and enhance security compliance.<br><br>These activities in the NIST CSF application as are a combination of a Target, Function, and Category. NIST CSF activities evaluate cybersecurity requirements for Targets, which provides detailed insights into gaps, non-compliant controls, risks, issues, failed indicators, and action plans and when they are addressed. Also, they help organizations strengthen their security compliance position. |
| Functions | Functions organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They help an organization by organizing information, enabling risk management decisions, addressing threats, and learning from previous activities to improve its management of cybersecurity risk.<br><br>In NIST CSF, functions select relevant cybersecurity outcomes for activities and organize them. |
| Category | Categories are the subdivisions of functions that are broken into groups of cybersecurity |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Concept | Description |
| --- | --- |
| | outcomes. Examples of categories include: Asset Management, Identity Management and Access Control, and Detection Processes.<br><br>Subcategories are used to divide a category into specific outcomes of technical and management activities. They provide a set of results that can help support achievement of the outcomes in each category. Examples of subcategories include: External information systems are cataloged, Data-at-rest is protected, and Notifications from detection systems are investigated.<br><br>The Framework Core identifies underlying categories and subcategories for each function as cybersecurity policies and their details as policy statements. The NIST CSF categories define the cybersecurity activities for targets and uses the associated subcategories to evaluate cybersecurity requirements to provide additional insight. |
| Implementation state | State of the cybersecurity activity, whether implemented or planned for the future. It is possible to document the implementation state of a cybersecurity activity. |
| Gaps | Control objectives of the cybersecurity policy that do not have any controls in-place for the target's profile identified in the cybersecurity activity. |
| Non-compliant controls | Cybersecurity controls that are considered non-compliant because of implementation issues and have been found for the target's entity, which is identified in the cybersecurity activity. |
| Risks | Risks associated with the controls implemented for the target's entity, which is identified in the cybersecurity activity. |
| Issues | Issues with controls and risks for the target's entity, which are identified in the cybersecurity activity. |
| Failed indicators | Failed indicators of controls and risks implemented for the target's entity, which is identified in the cybersecurity activity. |
| Action plans | Action plans for issues for the target's entity, which are identified in the cybersecurity activity. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### NIST CSF Use Case Accelerator dashboards and reports

The contains various reports. The NIST Cybersecurity Framework (CSF) Use Case Accelerator contains a variety of reports displayed on different dashboards, available within each of the sections in the NIST CSF process:

#### Overview reports

Repots available under **NIST CSF** > **Overview**.

| Reports | Purpose |
|---|---|
| Framework Core | Provides an overview of the Cybersecurity policies organized by the NIST CSF functions. |
| Critical Targets | Provides an overview of critical targets by entity class or tiers. |
| Critical Targets lacking Cybersecurity activities | Provides an overview of critical targets that lack cybersecurity activities by entity class or tiers. |
| Current Cybersecurity activities | Provides an overview of currently performed cybersecurity activities by entity class, entities, or cybersecurity functions. |
| Desired Cybersecurity activities | Provides an overview of desired cybersecurity activities by entity class, entities, or cybersecurity functions. |
| Gaps Analysis Summary | Provides a summary of gaps, non-compliant controls, risks, issues failed indicators, and action plans for targets grouped by cybersecurity, cybersecurity functions, or the targets themselves. |

#### Framework profiling reports

Reports available under **NIST CSF** > **Framework Profiling** > **Overview**.

| Reports | Purpose |
|---|---|
| Gaps | Displays an overview of the gaps that exist for cybersecurity activities. Gaps are grouped by policies, entity class, profiles, or functions. |
| Risks | Displays an overview of risks that exist for cybersecurity activities. Risks are grouped by policies, profile class, entities, or functions. |
| Non-compliant Controls | Displays an overview of non-compliant controls that exist for cybersecurity activities. Non-compliant controls are grouped by policies, entity class, profiles, or functions. |
| Failed Indicators | Displays an overview of failed indicators that for cybersecurity activities. Indicators are grouped by policies, entity class, entities, or functions. |
| Issues | Displays an overview of issues for cybersecurity activities. Issues are grouped by policies, entity class, entities, or functions. |
| Action Plans | Displays an overview of action plans that exist for cybersecurity activities. Action plans are grouped by policies, entity class, entities, or functions. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### NIST CSF process overview

The NIST CSF navigation structure facilitates the management of the NIST cybersecurity through activities of identification and the prioritization, as described in the NIST Framework for Improving Critical Infrastructure Cybersecurity version 1.1 special publication.

## NIST CSF process overview

1. The risk executives and/or the security officers identify categories and subcategories as cybersecurity policies.
2. The risk executives and/or the security officers prioritize cybersecurity activities.
3. Monitor the NIST CSF Overview dashboard

### Identify the framework core

Within the NIST CSF application, the **Framework Core** section is used to identify categories and subcategories as cybersecurity policies and their statement policies.

The application uses categories to define cybersecurity activities for targets and uses subcategories to evaluate cybersecurity requirements to provide additional details on compliance.

With NIST CSF guidance, the application groups categories and subcategories into functions and represent them as activities. The NIST CSF uses the following five modules to designate individual functions:

- Identify
- Protect
- Detect
- Respond
- Recover

Each module points to a grouping of policy and control objectives that relates to that function.

### Review the Framework Core

Review the Framework Core that's activated with the NIST CSF application.

### Before you begin

Role required: none.

Policy and Compliance Management role required: admin

NIST CSF role required: sn_irm_nist_csf.risk_executive or sn_irm_nist_csf.security_officer

### Procedure

1. Navigate to **All** > **NIST CSF** > **Framework Core** and then select one of the following modules:
   - **Identify**
   - **Protect**
   - **Detect**
   - **Respond**
   - **Recover**

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

2. In the Policy to Control Objectives form, click on one of the policy statements to review the information.

   **Note:** Policy statements are grouped by policies based on NIST CSF guidelines.

3. If necessary, update the record with additional information.
4. Click **Update**.

### Align and prioritize cybersecurity activities

Within the NIST CSF application, the **Framework Profiling** section is used to help an organization to align and prioritize its cybersecurity activities with its requirements, risk tolerances, and resources.

First, a target is created from a entity or entity type. The application flow begins at **Orient Targets**. The user locates a target and sets it up for use with NIST CSF providing basic information. Next, the user identifies if the target is critical and establishes a tier for the target per NIST guidelines.

**Note:** NIST recommends focusing on critical targets for prioritizing the Cybersecurity risks.

Next, users log their cybersecurity activities. The activities require users to identify targets, functions, and categories that are associated with it.

**Note:** These activities are uniquely created to avoid creating duplicate activities for the same targets.

As the activities are created, users then determine the implementation state of these activities.

Next, users perform gap analysis on the cybersecurity activities. The analysis gives a detailed insight into the security position and evaluates the target for a specific cybersecurity activity.

The ServiceNow® GRC suite of applications play a crucial role in tracking the data that enables these metrics. The NIST CSF application is designed to provide the Cybersecurity framework, but it is completely enabled by the ServiceNow® GRC product.

### Generate a target for an entity

Generate a target record for an entity to track NIST CSF attributes for that entity.

#### Before you begin

Role required: admin, sn_irm_nist_csf.risk_executive or sn_irm_nist_csf.security_officer

#### Procedure

1. Generate a target for an entry.

   a. Navigate to **Policy and Compliance** > **Scoping** and select one of the following modules:

      - **Entity Types**
      - **My Entities**
      - **All Entities**

   b. Select one of the records.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

c. From the Entity form, click **Generate target**.

> **Note:** When you click Generate target, it generates the target only if the entity has not been used for other frameworks, such as GDPR DPIA.

d. Click **Update**.

2. Identify the target.
   a. Navigate to **NIST CSF** > **Framework Profiling** > **Orient Targets**.
   b. Search for the target using the **Name** or **Profile** fields.
   c. Confirm that the target appears in the list.

### Set up target for NIST CSF framework

Set up a target record to use with NIST CSF framework after you've identified a target.

#### Before you begin

Role required: none.

NIST CSF role required: sn_irm_nist_csf.risk_executive or sn_irm_nist_csf.security_officer

#### Procedure

1. Navigate to **All** > **NIST CSF** > **Framework Profiling** > **Orient Targets**.
2. Search for the target using the **Name** or **Profile** fields.
3. Open the target record.
4. Click the **Framework** field and select **NIST CSF**.
5. Click **Update**.
6. In the Targets list, open the record again.
7. Verify the information in the Target form.
8. In the NIST CSF section, fill out the fields (see table for field descriptions).

| Field | Description |
|---|---|
| Critical | Check box that indicates the target is focused on during cyber risks. NIST CSF recommends that organizations prioritize cybersecurity activities for critical targets |
| Tier | Tier for a target that describes its capability to address cyber risks. |

9. Click the **Activities** related list and validate the activities that are associated with the target.

### Orient target

After you've identified a target, orient the target to use with the NIST CSF framework.

#### Before you begin

Role required: none.

Policy and Compliance Management role required: admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

NIST CSF role required: sn_irm_nist_csf.risk_executive or sn_irm_nist_csf.security_officer

### Procedure

1. Navigate to **All** > **NIST CSF** > **Framework Profiling** > **Orient Targets**.
2. Search for the target using the **Name** or **Profile** fields.
3. Open the record.
4. Verify that the **Framework** field has **NIST CSF** selected.
5. Ensure that the NIST CSF form fields are accurate.
6. Click **Update**.

## Create activity

Create a cybersecurity activity for a target.

### Before you begin

Role required: none.

Policy and Compliance Management role required: admin

NIST CSF role required: sn_irm_nist_csf.risk_executive or sn_irm_nist_csf.security_officer

### Procedure

1. Navigate to **All** > **NIST CSF** > **Framework Profiling** > **Create Activity** and create a new record (see table for field descriptions).

**NIST CSF Activity form**

| Field | Description |
|---|---|
| Number | Number that identifies the activity. |
| Target | Name of the target that has the activity associated with it. |
| Function | Type of function activities are grouped in. |
| Category | Cybersecurity activity that is identified as a policy. |
| Implementation state | Status of the activity, whether it is being performed or a planned activity. |

2. Click **Submit**.

**Note:** Every time a cybersecurity activity is created, the system validates the combination of target, function, and category for uniqueness.

## Perform Gap analysis

Perform a Gap analysis of cybersecurity activities.

### Before you begin

Role required: none.

Policy and Compliance Management role required: admin

NIST CSF role required: sn_irm_nist_csf.risk_executive or sn_irm_nist_csf.security_officer

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

**Note:** The Gap analysis process should not take more than a minute. A weekly job that runs the gap analysis for users so the metrics are up-to-date.

### Procedure

1. Navigate to **All** > **NIST CSF** > **Framework Profiling** > **Gap Analysis**.
2. Search for the target using the **Name** or **Profile** fields.
3. Open the target record.
4. Click the **Activities** related list and select the activity.
5. Review the activity and click **Gap Analysis** to initiate the Gap analysis.
6. To view control objectives for the cybersecurity policy that do not have any controls in-place for the target's profile, click the **Gaps** related list.
7. To view issues with cybersecurity controls that are non-compliant because of implementation issues, click the **Non-compliant controls** related list.
8. To view Failed indicators of controls and risks for the target's profile, click the **Failed Indicators** related list.
9. To view risks associated with controls for the target's profile, click the **Risks** related list.
10. To view issues related to the controls and risks for the target's profile, click the **Issues** related list.
11. To view action plans for the target's profile, click the **Action Plans** related list.
12. Click **Save**.

#### Review action plan

Review the remediation tasks created for the controls or risks associated with cybersecurity activities. You can only edit or update action plans if you have sufficient privileges for the GRC suite.

### Before you begin

Role required: none.

Policy and Compliance Management role required: admin

NIST CSF role required: sn_irm_nist_csf.risk_executive or sn_irm_nist_csf.security_officer

### About this task

Action plans are typically created in the ServiceNow® GRC product through the Policy and Compliance Management, Risk Management, or Audit Management applications.

### Procedure

1. Navigate to **All** > **NIST CSF** > **Framework Profiling** > **Action Plan**.
2. Search for an action plan using parameters, such as issue, control, or risk, that are associated it.
3. Open the record.
4. Review the action plan.

## NIST RMF Use Case Accelerator

The NIST RMF Use Case Accelerator gives customers an operational head-start when adopting the NIST RMF. When the accelerator is downloaded and activated in the GRC

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

applications, pre-configured policies, scopes (profile, profile type recommendations), indicators, risks and other GRC elements appear.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

## Who uses the NIST RMF Use Case Accelerator

| Persona | Description |
|---|---|
| Risk executive | Ensures that risks are identified and managed consistently across the organization.<br><br>Defined access to the following sections:<br>• **NIST RMF** > **Overview**<br>• **NIST RMF** > **Categorize**<br>• **NIST RMF** > **Select**<br>• **NIST RMF** > **Implement**<br>• **NIST RMF** > **Assess**<br>• **NIST RMF** > **Authorize**<br>• **NIST RMF** > **Monitor**<br>• **NIST RMF** > **Content** |
| Authorizing officer | Confirms that a target is operating within an acceptable level of risk.<br><br>Defined access to the following sections:<br>• All Modules in **NIST RMF** > **Overview** ><br>• **NIST RMF** > **Authorize** > **Targets**<br>• **NIST RMF** > **Authorize** > **My Approvals** |
| Security officer | Provides insight and understanding into the current security procedures and capabilities for a target and implements the controls, managing issues, and completing remediation tasks<br><br>Defined access to the following sections:<br>• **NIST RMF** > **Categorize**<br>• **NIST RMF** > **Select** > **Targets**<br>• **NIST RMF** > **Implement**<br>• **NIST RMF** > **Assess** > **Overview**<br>• **NIST RMF** > **Assess** > **Control Attestations**<br>• **NIST RMF** > **Assess** > **Control Effectiveness**<br>• **NIST RMF** > **Assess** > **Remediation Tasks**<br>• **NIST RMF** > **Authorize**<br>• **NIST RMF** > **Monitor** |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Persona | Description |
|---|---|
| Control provider | Assists in the creation and tailoring of security controls within the organization.<br>Defined access to the following sections:<br>• **NIST RMF** > **Select** > **Review Baseline Controls**<br>• **NIST RMF** > **Select** > **Tailor Baseline Controls**<br>• **NIST RMF** > **Content** |
| Sys admin | Access to the following sections: **NIST RMF** > **Administration** |
| GRC admin | Access to the following sections: **NIST RMF** > **Administration** |

### Install the NIST RMF Use Case Accelerator

The NIST RMF Use Case Accelerator is used with the GRC core applications: Policy and Compliance Management, Risk Management, and Audit Management applications.

**Before you begin**
Role required: none.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Complete the following setup checklist prior to installation. These setup tasks are required for a smooth installation.

| Setup task | Description |
|---|---|
| Verify that the following applications have been installed:<br>• Policy and Compliance Management<br>• Risk Management<br>• Audit Management | To verify that these applications are activated, navigate to **Subscription Management** > **Subscriptions** in your instance. The list displays the subscriptions your organization has purchased.<br>For more information about the setup and activation of the Risk Management plugin, see Install Risk Management |
| Verify that you have the required roles. | The System Admin (admin) assigns the following roles:<br>• Policy and Compliance Management roles<br>◦ Attestation Creator (sn_compliance.attestation_creator)<br>◦ Compliance Administrator (sn_compliance.admin) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Setup task | Description |
| --- | --- |
| | ◦ Compliance Developer (sn_compliance.developer)<br>◦ Compliance Manager (sn_compliance.manager)<br>◦ Compliance Reader (sn_compliance.reader)<br>◦ Compliance User (sn_compliance.user)<br>• Risk Management roles<br>◦ Risk Admin (sn.risk.admin)<br>◦ Risk Reader (sn.risk.reader)<br>◦ Risk Manager (sn.risk.manager)<br>◦ Risk User (sn.risk.reader)<br>• Audit Management roles<br>◦ Audit Admin (sn_audit.admin)<br>◦ Audit Developer (sn_audit.developer)<br>◦ Audit Manager (sn_audit.manager)<br>◦ Audit User (sn_audit.user)<br>◦ External Auditor (sn_audit.external_auditor) |

### Procedure

1. Log in to the instance you want to install the application on.
2. Navigate to **System Applications** > **All Available Applications** > **All**.
3. Locate the **GRC: NIST RMF Accelerator** application.
4. If you want to load demo data, select the **Demo Data** check box.
5. Click **Install**.

#### Verify the NIST RMF Use Case Accelerator

After installing the GRC: NIST RMF Use Case Accelerator, review the NIST RMF application structure, core content, and demo data, if selected during installation.

### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **User Administration** > **Roles** and review the roles installed with the NIST RMF application.

   These roles contain nist_rmf in their names; for example, sn_irm_nist_rmf.security_officer. The roles are associated with NIST RMF application modules to provide access based on the user's role.

   **Note:** Use the basic NIST RMF user role is to access the application. This role contains the reader or user roles from the ServiceNow® GRC suite of applications.

2. In the Application Navigator, type **NIST RMF**, and verify the application core content.

| Navigate to | Verify |
|---|---|
| **NIST RMF** > **Content** > **Control Objective** | Review the Policies and Control objectives installed for NIST RMF. |
| **NIST RMF** > **Content** > **Risk Statements** | Review the Risk Frameworks and Risk Statements installed for NIST RMF. |
| **NIST RMF** > **Content** > **Test Templates** | Review the Test Templates installed for NIST RMF. |
| **NIST RMF** > **Content** > **Indicator Templates** | Review the Indicator Templates installed for NIST RMF. |
| **NIST RMF** > **Content** > **Attestation Types** | Review the Control Attestation Types installed for NIST RMF. |
| **NIST RMF** > **Content** > **Assessment Types** | Review the Risk Assessment Types installed for NIST RMF. |

3. Validate the application demo content, if loaded.

| Navigate to | Verify |
|---|---|
| **NIST RMF** > **Impact Analysis** | Review the sample Targets installed in the system for use with the NIST RMF application. |
| **User Administration** > **Users** | Review the sample Persona users installed in the system for use with the NIST RMF application. The User IDs for these users end with .RMF and their names contain RMF. |
| **Policy and Compliance** > **Scoping** > **Profile Classes** | Perform a search for profile classes with the **Name** field containing **with NIST**. Review their relationships by reviewing their roll up to field in respective profile classes. |
| **Policy and Compliance** > **Scoping** > **Profile types** | Perform a search for profile types with the **Name** field starting with **NIST RMF**. |
| **Policy and Compliance** > **Policies and Procedures** > **All Controls** | Perform a search for all controls referencing **Control Objectives** with a **Source = NIST 800-53-r4**. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Navigate to | Verify |
|---|---|
| **Risk** > **Risk Register** > **All Risks** | Perform a search for all risks referencing **Risk Statements** with a **Source = NIST 800-53-r4**. |
| **Audit** > **Audit Testing** > **Test Plans** | Perform a search for test plans with **Test Templates** that begin with **NIST RMF**. |
| **Policy and Compliance** > **Indicators** > **Indicators** | Perform a search for all indicators where **Item.Content.Source = NIST 800-53-r4**. |
| **Risk** > **Indicators** > **Indicators** | Perform a search for all indicators where **Item.Content.Source = NIST RMF**. |
| **Policy and Compliance** > **Issues** > **All Issues** | Perform a search for all issues where**Item.Content.Source = NIST 800-53-r4**. |
| **Risk** > **Issues** > **All Issues** | Perform a search for all issues where **Item.Content.Source = NIST 800-53-r4**. |
| **Policy and Compliance** > **Remediation Tasks** > **All Open Remediation Tasks** | Perform a search for all Remediation tasks where an issue identified on the remediation task has**Item.Content.Source = NIST 800-53-r4**. |
| **Risk** > **Remediation Tasks** > **All Open Remediation Tasks** | Perform a search for all Remediation tasks where an issue identified on the remediation task has **Item.Content.Source = NIST 800-53-r4**. |

### NIST RMF supporting concepts

Familiarize yourself with these concepts, developed from the NIST RMF guidance.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

| Concept | Description |
|---|---|
| Target | The target is the foundation of the NIST RMF Use Case Accelerator and all related concepts.<br><br>The target is a shared table between the ServiceNow® GRC products and several Use Case Accelerators. They are similar to the concept of profiles in the core GRC applications. They are optionally linked to profiles, but are used for any attributes that are specific to the Use Case Accelerators.<br><br>**Note:** Each NIST RMF Target uniquely represents a single profile throughout its RMF life-cycle. |
| Confidentiality (C) | Confidentiality is a security objective of a Target, and is defined as the act of preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Confidentiality is expressed as High, Moderate, and Low values |
| Integrity (I) | Integrity is a security objective of a Target is defined as act of guarding against improper information modification or destruction, and includes |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Concept | Description |
|---|---|
| | ensuring information non-repudiation and authenticity. Integrity is expressed as High, Moderate, and Low values |
| Availability (A) | Availability is a security objective of a Target is defined as act of ensuring timely and reliable access to and use of information. Availability is expressed as High, Moderate, and Low values |
| Baseline controls | Baseline Controls are recommended set of security controls from National Institute of Standards and Technology (NIST) which when implemented and determined to be effective, would mitigate security risk while complying with security requirements. Baseline controls have a designated impact value which is a combination of High, Moderate, or Low values. |
| Impact analysis | Impact analysis determines the extent to which proposed or actual changes to the Target or its environment of operation can affect or have affected the security state of the Target. A Target in which all three CIA security objectives evaluate to Low is considered Low-impact and uses any of the security controls which are tagged as Low impact value. Likewise, a Target in which any of the three CIA security objectives evaluate to Moderate is considered Moderate-impact and uses any of the security controls which are tagged as Moderate impact value. Likewise, a Target in which any of the three CIA security objectives evaluate to High is considered High-impact and uses any of the security controls which are tagged as High impact value. |
| Assurance | Assurance controls increase both the strength of security and degree of confidence that the functionality of Targets is correct, complete, and consistent and would mitigate the security risk and assists in complying with security requirements |
| Common | Common controls are controls that are inheritable by one or more Targets |
| Compensating | Compensating controls are controls which can be employed in lieu of recommended baseline security controls and provide equivalent or comparable protection for the Targets |
| Supplemental | Supplemental controls are controls which can be employed as added security controls to adequately meet the risk management needs of a Target |
| Tailoring | Tailoring is a process by which a security control baseline is modified based on: (i) Targets scoping guidance; (ii) specification of the security controls, for example, compensating, if needed; and (iii) the specification of organization — defined parameters in the security controls via explicit assignment and selection statements |

### NIST RMF Use Case Accelerator dashboards and reports

The NIST RMF Use Case Accelerator contains various reports displayed on different dashboards, available within each of the sections in the NIST RMF process: Categorize, Select, Implement, Assess, Authorize, and Monitor.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Overview reports

Reports under **NIST RMF** > **Overview**.

| Reports | Purpose |
|---|---|
| Security Compliance Overview | Provides an overall compliance summary of the security policies. |
| Profiles Compliance Overview | Provides an overall compliance summary of the profiles implementing security controls. |
| Security Compliance Details | Provides a detailed compliance summary of the security policies. |
| Inherent Security Risk Heatmap | Heatmap of security risks based on the Inherent qualitative results of risks. |
| Residual Security Risk Heatmap | Heatmap of security risks based on the Residual qualitative results of risks. |
| Inherent Security Risk | Bubble chart of security risks based on the average Inherent quantitative results of risks. |
| Residual Security Risk | Bubble chart of security risks based on the average Inherent quantitative results of risks. |
| Inherent Annual Loss Exposures Security Risk | Provides an insight into Inherent Annualized Loss Expectancy (ALE) for different security risks. |
| Residual Annual Loss Exposures Security Risk | Provides an insight into Residual Annualized Loss Expectancy (ALE) for different security risks. |
| Issues summary | Plots issues noted for security policies on a week by week basis. |

### Categorize reports

Reports under **NIST RMF** > **Categorize** > **Overview**.

| | |
|---|---|
| Targets with no Baseline Controls | Targets with completed security impact analysis with no baseline control generated. Baseline Controls are recommended set of security controls from National Institute of Standards and Technology (NIST) which when implemented and determined to be effective, would mitigate security risk while complying with security requirements. The Baseline Controls to be implemented can be determined from the recommended Baseline Policy Statements on the Target. |
| Targets pending Impact Analysis | Security impact analysis when conducted by the organizations, determines the extent to which proposed or actual changes to the target or its environment of operation can affect or have affected the security state of the target. Changes to the target or its environment of operation may affect the security controls currently in place (including system-specific, hybrid, and common controls), produce new vulnerabilities in the target, |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Categorize reports**

Reports under **NIST RMF** > **Categorize** > **Overview**.

**(continued)**

| | |
|---|---|
| | or generate requirements for new security controls that were not needed previously. |
| Targets status | Targets organized by their current state of Risk Management process. The Risk Management process is provided by National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is a disciplined and structured process that integrates information security and risk management activities. |
| Confidentiality Impact | Targets grouped for each confidentiality rating value. National Institute of Standards and Technology (NIST) defines Confidentiality as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Confidentiality is expressed as High, Moderate, and Low values. |
| Integrity Impact | Targets grouped for each Integrity rating value. National Institute of Standards and Technology (NIST) defines Integrity as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Integrity is expressed as High, Moderate, and Low values. |
| Availability Impact | Targets grouped for each Availability rating value. National Institute of Standards and Technology (NIST) defines Availability as ensuring timely and reliable access to and use of information. Availability is expressed as High, Moderate, and Low values. |
| Impact | Targets grouped for each Impact rating value. National Institute of Standards and Technology (NIST) defines Impact as the loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect; (ii) a serious adverse effect; or (iii) a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Whereas security impact analysis is defined as organizations determination of the extent to which the security state is affected. Impact is expressed as High, Moderate, and Low values. |
| Review Baseline Controls | Provides an overview for the NIST Risk Management select step of the framework in-order to facilitate review of the baseline policy statements and controls. NIST RMF > Select > Review Baseline Controls launches this dashboard |
| Baseline Security Policy Statements | Baseline Security Policy Statements are recommended set of security control definitions from National Institute of Standards and Technology (NIST) which when implemented and determined to be effective, would mitigate security risk while complying with security requirements. |
| Baseline Security Controls | Baseline Security Controls are recommended set of security controls from National Institute of Standards and Technology (NIST) which are being implemented and if determined to be effective, would mitigate security risk while complying with security requirements. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Baseline control reports

Reports under **NIST RMF** > **Select** > **Review Baseline Controls**.

| Reports | Purpose |
|---|---|
| Baseline Security Policy Statements | Baseline Security Policy Statements are recommended set of security control definitions from National Institute of Standards and Technology (NIST) which when implemented and determined to be effective, would mitigate security risk while complying with security requirements. |
| Baseline Security Controls | Baseline Security Controls are recommended set of security controls from National Institute of Standards and Technology (NIST) which are being implemented and if determined to be effective, would mitigate security risk while complying with security requirements. |

### Tailor baseline controls reports

Reports under **NIST RMF** > **Select** > **Tailor Baseline Controls**.

| Reports | Purpose |
|---|---|
| Baseline Assurance Policy Statements | Baseline Security Assurance Policy Statements are recommended set of security control definitions from National Institute of Standards and Technology (NIST) which are designated as Assurance control definitions which when implemented increase both the strength of security and degree of confidence that the functionality is correct, complete, and consistent and would mitigate security risk while complying with security requirements. |
| Baseline Assurance Controls | Baseline Security Assurance Controls are recommended set of security control definitions from National Institute of Standards and Technology (NIST) which are designated as Assurance control are being implemented to increase both the strength of security and degree of confidence that the functionality is correct, complete, and consistent and would mitigate security risk while complying with security requirements. |
| Baseline Common Policy Statements | Baseline Security Common Policy Statements are set of security control definitions from National Institute of Standards and Technology (NIST) which when designated as Common control definitions by organizations indicate these are inheritable by one or more organizational targets. |
| Baseline Common Controls | Baseline Security Common Controls are set of security control definitions from National Institute of Standards and Technology (NIST) are being implemented and which when designated as Common controls by organizations indicate these are inheritable by one or more organizational targets. |
| Baseline Compensating Policy Statements | Baseline Security Compensating Policy Statements are set of security control definitions from National Institute of Standards and Technology (NIST) which when designated as Compensating control definitions by organizations indicate these can be employed in lieu of other security controls and provide equivalent or comparable protection for organizational targets. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Tailor baseline controls reports

Reports under **NIST RMF** > **Select** > **Tailor Baseline Controls**.

**(continued)**

| Reports | Purpose |
|---|---|
| Baseline Compensating Controls | Baseline Security Compensating Controls are set of security control definitions from National Institute of Standards and Technology (NIST) are being implemented and which when designated as Compensating controls by organizations indicate these can be employed in lieu of other security controls and provide equivalent or comparable protection for organizational targets. |
| Baseline Supplemental Policy Statements | Baseline Security Supplemental Policy Statements are set of security control definitions from National Institute of Standards and Technology (NIST) which when designated as Supplemental control definitions by organizations indicate these can be added to security controls to adequately meet the risk management needs for organizational targets. |
| Baseline Supplemental Controls | Baseline Security Supplemental Controls are set of security control definitions from National Institute of Standards and Technology (NIST) are being implemented and which when designated as Supplemental controls by organizations indicate these can be added to security controls to adequately meet the risk management needs for organizational targets. |

### Attestation and assessment reports

Reports under **NIST RMF** > **Assess** > **Overview**.

| Reports | Purpose |
|---|---|
| Control Attestations completed | Displays the number of NIST Risk Management control attestations completed. |
| Control Attestations upcoming due date | Displays the number of NIST Risk Management control attestations due within 7 days. |
| Control Attestations due after 7 days | Displays the number of NIST Risk Management control attestations due after 7 days. |
| Control Attestations missed due date | Displays the number of NIST Risk Management control attestations that have missed their due date. |
| Control Attestations by profile | Provides an overview of the NIST Risk Management control attestations grouped by profiles. |
| Control Attestations past due | Provides an overview of the NIST Risk Management control attestations grouped by due date. |
| Risk Assessments completed | Displays the number of NIST Risk Management risk assessments completed. |
| Risk Assessments upcoming due date | Displays the number of NIST Risk Management risk assessments due within 7 days. |
| Risk Assessments due after 7 days | Displays the number of NIST Risk Management risk assessments due after 7 days. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Attestation and assessment reports

Reports under **NIST RMF** > **Assess** > **Overview**.

**(continued)**

| Reports | Purpose |
|---|---|
| Risk Assessments missed due date | Displays the number of NIST Risk Management risk assessments that have missed their due date. |
| Risk Assessments by profile | Provides an overview of the NIST Risk Management risk assessments grouped by profiles. |
| Risk Assessments past due | Provides an overview of the NIST Risk Management risk assessments grouped by due date. |

### Approval reports

Reports under **NIST RMF** > **Authorize** > **Overview**.

| Reports | Purpose |
|---|---|
| Target approval status | Provides an overview of the current state of approvals of the target. |
| Risk Executive approvers | Provides an overview of targets as assigned to the risk executive approvers. |
| Authorizing Official approvers | Provides an overview of targets as assigned to the authorizing official approvers. |

### Monitoring reports

Reports under **NIST RMF** > **Monitor** > **Overview**.

| Reports | Purpose |
|---|---|
| In-effective Profiles | Total number of profiles having at least one control test of a security control flagged as in-effective. |
| In-effective Controls | Total number of security controls having atleast one control test flagged as in-effective. |
| In-effective Test Plans | Total number of test plans having at least one control test of a security control flagged as in-effective. |
| Non-compliant Controls | Total number of security controls with status non-compliant. |
| Risks | Total number of Risks that are associated with security controls. |
| Issues | Total number of issues that are related to security controls and risks. |
| Control compliance | Provides compliance overview of the security controls. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Monitoring reports

Reports under **NIST RMF** > **Monitor** > **Overview**.

**(continued)**

| Reports | Purpose |
|---|---|
| Profile effectiveness | Provides an overview of the profile effectiveness for profiles having security controls based on the effectiveness of the associated control tests. |
| Control effectiveness | Provides an overview of the control effectiveness for security controls based on the effectiveness of the associated control tests. |
| Test Plan effectiveness | Provides an overview of the test plan effectiveness of security controls based on the effectiveness of the associated control tests. |
| Risks | List of Risks grouped by profiles and associated with security controls. |

### NIST RMF process overview

The NIST RMF navigation structure facilitates the management of the NIST security controls through activities of categorization, selection, implementation, assessment, authorization, and monitoring. These security controls are described in the NIST 800-37.r1 special publication.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

## NIST RMF process overview

1. The risk executives and/or the security officers categorize the targets.
2. The risk executives, the security officers and/or the control providers select baseline control definitions.
3. The risk executives and/or the security officers implement baseline security controls.
4. The security accessors, the risk executives, and/or the security officers assess the security controls:
   a. Manage and address issues
   b. Manage and address remediation tasks
5. The authorizing official, the risk executives, and/or the security officers authorize targets.
6. The risk executives and/or the security officers monitor security controls:
   a. Review and manage indicators
   b. Monitor the NIST RMF Overview dashboard

### Categorize targets

Within the NIST RMF application, the **Categorize** section facilitates the categorization of targets through a preliminary risk assessment and an impact analysis.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

First, a target is created from an entity or an entity type. The application flow begins at Impact Analysis. The user locates a target and sets it up for use with NIST RMF providing basic information. Next, the user performs a preliminary risk assessment determining the potential impact value on each of the following parameters: **Confidentiality**, **Integrity**, and **Availability**. The highest impact rating of these values determines the **Impact** value.

**Note:** The user can override the **Impact** value, as necessary.

The **Impact** value is used to identify the baseline security policy statements recommended for the target, based on the NIST 800-53.r4 special publications catalog. The user reviews the baseline security policy statements and implements security controls for that target (for example, Profile). The standard approach is outlined in the Policy and Compliance Management application.

### Generate target from profile or entity type

Generate a target record for a profile to track NIST RMF attributes.

#### Before you begin

Role required: none.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Policy and Compliance Management role required: admin

NIST RMF role required: sn_irm_nist_rmf.risk_executive or sn_irm_nist_rmf.security_officer

#### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Scoping** > **Profile Types**
   - **Policy and Compliance** > **Scoping** > **My Profile**
   - **Policy and Compliance** > **Scoping** > **All Profiles**
2. Select and open Profile Type of Profile record.
3. Check **Generate Target** and click **Update**.
4. Identify the target:
   a. Navigate to **NIST RMF** > **Categorize** > **Impact Analysis**.
   b. Search for the target using the **Name** or **Profile** fields.
   c. Confirm that the target appears in the list.

### Set up a target for use with NIST RMF

Set up a target and populate the basic information.

#### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.risk_executive or sn_irm_nist_rmf.security_officer

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **NIST RMF** > **Categorize** > **Impact Analysis**.
2. Search for the target using the **Name** or **Profile** fields.
3. Open the target record.
4. In **Framework**, select **NIST RMF**, and click **Update**.
5. Open the target record again and update the following fields:

   **Note:** Review NIST RMF supporting concepts, for more detailed information about these fields.

   - **RMF State**: Identify the current NIST RMF state for the target.
   - **Scoping Considerations**: Provide guidance on the selection of security controls for implementation.
6. Verify that the NIST RMF related lists are visible:
   - Baseline Policy Statements
   - Baseline Controls
   - Risks
   - Approvals

#### Perform preliminary risk assessment and impact analysis

Perform a preliminary risk assessment and impact analysis of the target.

### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.risk_executive or sn_irm_nist_rmf.security_officer

### Procedure

1. Navigate to **All** > **NIST RMF** > **Categorize** > **Impact Analysis**.
2. Search for the target using the **Name** or **Profile** fields.
3. Select and open the target record.
4. Open the target record again and update the following fields in the NIST RMF section:

   **Note:** Review NIST RMF supporting concepts, for more detailed information about these fields.

#### NIST RMF section

| Field | Description |
|---|---|
| Confidentiality | Target category based on confidentiality. Identify the security objective as: High, Moderate, or Low. |
| Integrity | Target category based on integrity. Identify the security objective as: High, Moderate, or Low. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Availability | Target category based on availability. Identify the security objective as: High, Moderate, or Low. |
| Impact | Impact to business function if the target loses its confidentiality, integrity, or availability. Impact is automatically determined and may be overridden. |
| Scoping Considerations | Operational or environmental scoping considerations for the target. |
| Risk Executive | Names of the person who ensures risks are identified and managed. |
| Authorizing Official | Name of the person who verifies that the target is operating with an acceptable level of risk. |
| Justification | Security posture description for risk executive, authorizing official, and owner. |
| Approval status | Status of the security compliance posture of the target. |

5. Verify that the NIST RMF related lists are visible:
   - Baseline Policy Statements
   - Baseline Controls
   - Risks
   - Approvals
6. Navigate to the **NIST RMF** tab and review the **Baseline Policy Statements**.
7. Implement security controls for the target following the standard approach outlined in the Policy and Compliance Management application.

### Monitor the NIST RMF Categorize Overview

The NIST RMF categorization activity dashboard provides insights into the overall status of the target.

#### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.risk_executive or sn_irm_nist_rmf.security_officer

#### Procedure

1. Navigate to **All** > **NIST RMF** > **Categorize** > **Overview**
2. Review all the reports on the dashboard.
3. Review the report details in the dashboard and reports sections.

### Select baseline control definitions

Within the NIST RMF application, the **Select** section focuses on the review of the initial set of baseline control definitions. You can also tailor the control definitions, by tagging them based on organizational requirements.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

After performing **Impact Analysis**, the user selects and tailors the baseline controls for that target. A dashboard provides an overview of the baseline policy statements in the catalog, alongside the catalog of baseline controls being implemented.

Next, the user tailors the baseline controls. Another dashboard contains several reports detailing the baseline policy statements alongside baseline controls which are tagged as **Assurance**, **Common**, **Compensating** and **Supplemental**.

**Note:** Both **Review Baseline Controls** and **Tailor Baseline Controls** require that you implement all necessary controls following the standard Policy and Compliance Management application procedures. Return to these dashboards for the selecting and tailoring of those controls.

### Review baseline controls

Review the baseline policy statements and baseline controls.

#### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

**Review Baseline Controls** requires that you implement all necessary controls following the standard Policy and Compliance Management application procedures.

Role required: sn_irm_nist_rmf.risk_executive, sn_irm_nist_rmf.security_officer, or sn_irm_nist_rmf.control_provider

#### Procedure

1. Navigate to **All** > **NIST RMF** > **Select** > **Review Baseline Controls**.
2. Review all the reports on the dashboard.
3. Implement changes for the baseline policy statements and baseline controls following the standard approach outlined Policy and Compliance Management application.

### Tailor baseline controls

Tailor the baseline policy statements and baseline controls.

#### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

**Tailor Baseline Controls** requires that you implement all necessary controls following the standard Policy and Compliance Management application procedures.

Role required: sn_irm_nist_rmf.risk_executive, sn_irm_nist_rmf.security_officer, or sn_irm_nist_rmf.control_provider

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **All** > **NIST RMF** > **Select** > **Tailor Baseline Controls**.
2. Review all the reports on the dashboard.
3. Implement changes for the baseline policy statements and baseline controls following the standard approach outlined in the Policy and Compliance Management application.

### Implement security controls

Within the NIST RMF application, the **Implement** section focuses on the physical implementation of the baseline security controls. The NIST RMF application may also include other standard security controls, already used by the targets or its environment of operation.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Users can view a list of all controls that originate from a NIST 800-53.r4 policy statement, update any implementation details, and update the controls.

**Note:** The NIST RMF application provides read-only access to the security controls. Update these controls following the standard Policy and Compliance Management application procedures.

An important aspect of implementing controls is testing them appropriately. Users can view a list of all control tests that were created for security controls with a policy statement source of NIST 800-53 r4.

**Note:** The NIST RMF application provides read-only access to the security control tests. Update these tests following the standard Audit Management application procedures.

### Manage and implement controls

From a list of security controls stemming from NIST 800-53.r4 policy statements, review the controls and update implementation details.

## Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.risk_executive or sn_irm_nist_rmf.security_officer

## Procedure

1. Navigate to **All** > **NIST RMF** > **Implement** > **Active Controls**.
2. Review each control and physically implement them following the standard approach outlined in the Policy and Compliance Management application.

### Manage and implement control tests

From a list of security controls stemming from NIST 800-53.r4 policy statements, review the control tests and update implementation details.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.risk_executive or sn_irm_nist_rmf.security_officer

### Procedure

1. Navigate to **All** > **NIST RMF** > **Implement** > **Active Control Tests**.
2. Review each control test and physically implement them following the standard approach outlined in the Audit Management application.

#### Assess controls, risks, issues, and remediation tasks

Within the NIST RMF application, the **Assess** section involves performing security control attestations, evaluating the control effectiveness, managing associated risks and issues, and performing remediation tasks.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Broadly, assessment also involves managing the controls, risks, issues, and remediation tasks that stem from the implementation of the security controls.

**Note:** The NIST RMF application provides read-only access to the content. Update the content following the standard GRC procedures, as outlined in the Policy and Compliance Management, Risk Management, and/or Audit Management applications.

Users can:

- review and perform control attestations currently in the system relating to NIST RMF security attestations
- view all control tests, highlighting the control and current effectiveness of each control test in place
- manage and address any risks stemming from risk statements having a content source of NIST 800-53.r4
- identify risks and perform their assessments
- view a list of issues and remediation tasks stemming from the implementation of security controls and related risks having a content source of NIST 800-53 r4

#### Review and perform control attestations

Review and perform control attestations relating to NIST RMF security attestations.

### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.security_accessor, sn_irm_nist_rmf.risk_executive, or sn_irm_nist_rmf.security_officer

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

1. Navigate to **All** > **NIST RMF** > **Assess** > **Control Attestations**.
2. Review each control attestation and its results.
3. Perform any control attestations assigned to you following the standard approach outlined in the Policy and Compliance Management application.

#### Review and evaluate control effectiveness

Review and evaluate the effectiveness of the controls through the execution of control tests related to NIST-800.53.r4.

### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.security_accessor, sn_irm_nist_rmf.risk_executive, or sn_irm_nist_rmf.security_officer

### Procedure

1. Navigate to **All** > **NIST RMF** > **Assess** > **Control Effectiveness**.
2. Review each control test and their related security controls.
3. Review the control effectiveness results in the system.
4. Perform the control tests assigned to you following the standard approach outlined in the Audit Management application.

#### Manage and address risks

Review and manage all risks stemming from risk statements having the content source of NIST 800-53.r4.

### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.security_accessor or sn_irm_nist_rmf.risk_executive

### Procedure

1. Navigate to **All** > **NIST RMF** > **Assess** > **Risks**.
2. Review each risk and their related risk statements.
3. Manage and address any risks following the standard approach outlined in the Risk Management application.

#### Review and perform risk assessments

Review and execute the risk assessments relating to NIST RMF security assessments.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.security_accessor or sn_irm_nist_rmf.risk_executive

### Procedure

1. Navigate to **All** > **NIST RMF** > **Assess** > **Risk Assessments**.
2. Review each risk assessment and its results.
3. Perform any risk assessments assigned to you following the standard approach outlined in the Risk Management application.

#### Manage and address issues

Review all issues stemming from controls and risks with NIST 800-53.r4 as the source and address them.

### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.security_officer or sn_irm_nist_rmf.risk_executive

### Procedure

1. Navigate to **All** > **NIST RMF** > **Assess** > **Issues**.
2. Review the issues with NIST 800-53.r4 as the source.
3. Manage and address any risks following the standard approach outlined in the Risk Management application.

#### Manage and address remediation tasks

Review all remediation tasks stemming from controls and risks with NIST 800-53.r4 as the source and address them.

### Before you begin

Role required: none.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

NIST RMF role required: sn_irm_nist_rmf.security_officer or sn_irm_nist_rmf.risk_executive

### Procedure

1. Navigate to **All** > **NIST RMF** > **Assess** > **Remediation tasks**.
2. Review the issues with NIST 800-53.r4 as the source.
3. Manage and address any risks following the standard approach outlined in the Risk Management application.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Monitor the NIST RMF Assess dashboard

The NIST RMF assess dashboard provides insights into the overall status of the target.

#### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.security_officer or sn_irm_nist_rmf.risk_executive

#### Procedure

1. Navigate to **All** > **NIST RMF** > **Assess** > **Overview**.
2. Review all the reports on the dashboard.
3. Review the report details in the dashboard and reports sections.

### Authorize targets

Within the NIST RMF application, the **Authorize** section involves the authorization of targets based on their compliance and risk posture.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Users request authorization from the appropriate parties directly from the target form.

### Authorize targets

Authorize a target record based on the overall security posture determined by the security officer.

#### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.security_official, sn_irm_nist_rmf.risk_executive, or sn_irm_nist_rmf.security_officer

#### Procedure

1. Navigate to **All** > **NIST RMF** > **Authorize** > **Targets**.
2. Search for the target using the **Name** or **Profile** fields.
3. Select and open the target record.
4. From the NIST RFM section, review the **Approval Status** field.
5. Click **Request Approval**.

#### Result

The approval is triggered for the target.
If you are an approver, use the **My Approvals** module to review the approval request.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Monitor the NIST RMF Authorize dashboard

The NIST RMF Authorize dashboard provides insights into the overall status of the target.

#### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.security_officer or sn_irm_nist_rmf.risk_executive

#### Procedure

1. Navigate to **All** > **NIST RMF** > **Authorize** > **Overview**.
2. Review all the reports on the dashboard.
3. Review the report details in the dashboard and reports sections.

### Monitor security controls

Within the NIST RMF application, the **Monitor** section involves the on-going monitoring of the security controls for targets documenting changes to them or their environments of operation, conducting security impact analyses of the associated changes, and reporting their security state to designated officials.

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Monitoring is a critical step in the RMF process. In-effective targets (profiles), controls, and test plans can be continuously monitored and their known risks and issues addressed. Security controls should be automatically monitored where possible using indicators, triggering alerts for remediation.

To continuously monitor a security control, users can use the indicator templates provided with the NIST RMF Use Case Accelerator application, by navigating to **NIST RMF** > **Content** > **Indicator Templates**. The sample indicator templates and indicators begin with **NIST**. Users must create new indicators beginning with **NIST** for monitoring the security controls.

### Review and manage indicators

Review all indicators that are set up for NIST and manage them to track their results.

#### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.risk_executive or sn_irm_nist_rmf.security_officer

#### Procedure

1. Navigate to **All** > **NIST RMF** > **Monitor** > **Indicators**.
2. Review all indicators beginning with NIST.
3. Search for the indicator using the **Name** field.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. Select and open the indicator record.
5. Review the record and click **Save**.

### Monitor the RMF Monitor dashboard

The NIST RMF monitor dashboard provides insights into the overall status of the target.

#### Before you begin

**Note:** Starting with version 10.1.0, the NIST RMF Use Case Accelerator will be supported only for customers who currently use the product. New and existing customers should consider using the GRC: Continuous Authorization Monitoring application. For details, Continuous Authorization and Monitoring.

Role required: sn_irm_nist_rmf.security_officer or sn_irm_nist_rmf.risk_executive

#### Procedure

1. Navigate to **All** > **NIST RMF** > **Monitor** > **Overview**.
2. Review all the reports on the dashboard.
3. Review the report details in the dashboard and reports sections.

## Technology Controls Monitoring Accelerator

The Technology Controls Monitoring Accelerator is a collection of pre-defined indicator templates designed to ease collection of data, and aid validation and continuous monitoring of technology controls. This application can be run with the Cybersecurity Controls Accelerator or as a standalone application.

The indicator templates contained in the Technology Controls Monitoring Accelerator are linked to specific ServiceNow® applications to allow compliance validation for standards and frameworks such as:

- ISO/IEC 27001
- ISO/IEC 27002
- CIS Controls

These packaged indicator templates have also been mapped to related common controls in the Unified Compliance Framework (UCF) to enable validation of controls across a wide range of regulations and industry standards. The indicator templates can be used to validate compliance with related control objectives in custom policies. You can monitor controls obtained via the CIS Controls™ or technology controls common to CIS or ISO 27002, even if you do not subscribe to the CIS Controls. Or you can use the indicators from the Technology Controls Monitoring Accelerator to monitor data coming from UCF.

## Continuous monitoring of CIS Controls™ v8

CIS Controls™ are a prioritized set of safeguards to mitigate the cyber-attacks against systems and networks. These controls are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS Controls™ v8 has been enhanced to continue supporting the modern systems and software such as cloud-based computing, virtualization, mobility, outsourcing as businesses shift their working model to fully cloud and hybrid environments.

Beginning with the Utah release, Technology Controls Monitoring Accelerator provides pre-packaged CIS v8 controls and indicator templates to monitor them along with its common controls mapped to various standards.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following enhancements are supported with CIS Controls ™ v8:

- Enable continuous monitoring of CIS Controls ™ v8 using the predefined indicator templates.
- Enable monitoring of common controls from ISO 27002, PCI DSS 4.0, NIST 800-53, NIST CSF, CSA CCM 4.0 mapped to CIS V8.

### Download the Technology Controls Monitoring Accelerator

Before you run the Technology Controls Monitoring Accelerator application in your instance, you must download it from the ServiceNow Store.

#### Before you begin

If you downloaded the Cybersecurity Controls Accelerator application, you can skip this procedure as this application was installed as a dependency to the Cybersecurity Controls Accelerator application.

Prior to running the Technology Controls Monitoring Accelerator application, you must download and activate the following GRC applications:

- GRC: Policy and Compliance Management
- GRC: Profiles

Role required: admin

#### Procedure

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

### Ensure that all the appropriate indicator templates are activated

When you download the GRC: Technology Controls Monitoring Accelerator application, all indicator templates are available, but they are not yet active. Before activating them, you need to ensure that you have the necessary applications activated and can access the tables that are mapped to the indicator templates.

#### Before you begin

Role required: admin

#### About this task

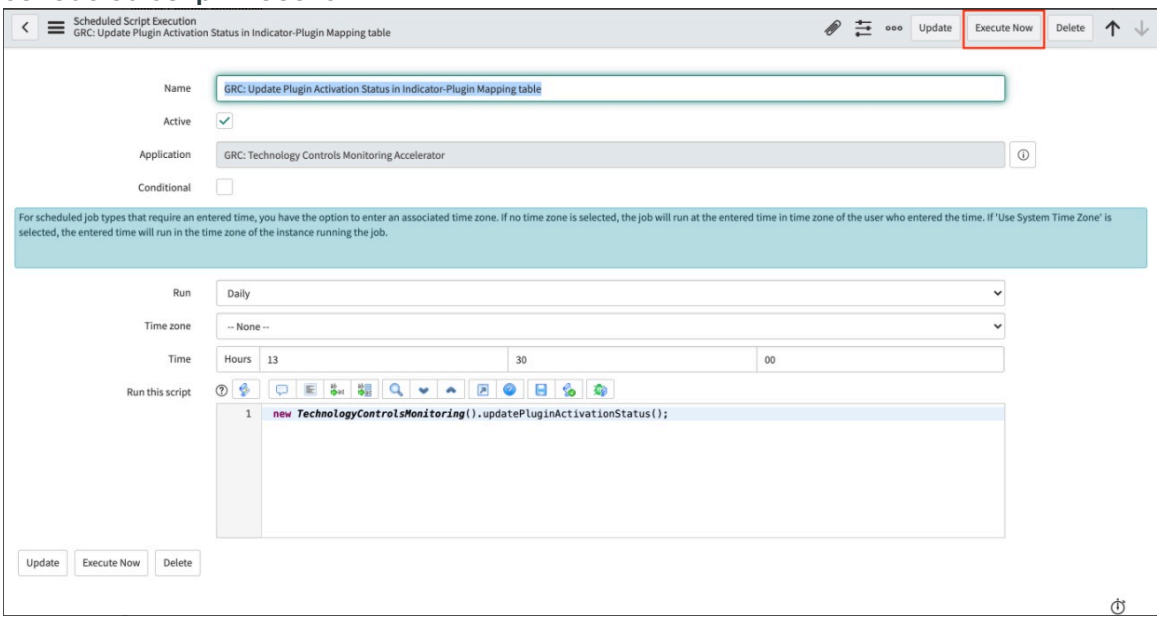
Starting with version 12.0.1 of the Technology Controls Monitoring Accelerator application, several of the indicators that were Manual were converted to either Basic or Scripted. This added automation makes many of the tasks associated with continuous monitoring easier.

#### Procedure

1. Navigate to **All** > **System Definition** > **Scheduled Jobs**.
2. Locate and open **GRC: Update Plugin Activation Status in Indicator-Plugin Mapping table**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Scheduled Script Execution




3. Click **Execute Now**.
   The job scans the Indicator Template to Plugin Mapping table [sn_grc_ind_template_plugin_mapping_details] on your instance, and 1) determines which applications that can use the Technology Controls Monitoring Accelerator for monitoring indicator templates are installed on your instance, and 2) automatically activates the indicator templates that are mapped to tables in those applications.

   **Note:** You must repeat this process any time you upgrade this application.

### View your operational status

View the Operational Status modules for a list of the CIS Controls and technology Controls. Each control also includes the technology used to validate compliance, type of indicator template available, and the control's source table.

#### Before you begin

Role required: admin or sn_compliance.reader

#### About this task

Starting with Version 12.0.2, the Operational Status modules provide a view of all of your CIS Controls and/or ISO 27002-based indicator templates mapped to specific CIS/ISO controls in one place. This information can be useful for monitoring your controls and the health of your system. The application is able to scan your instance and determine which controls you have implemented, along with the various technologies available for validating each control and protecting your data.

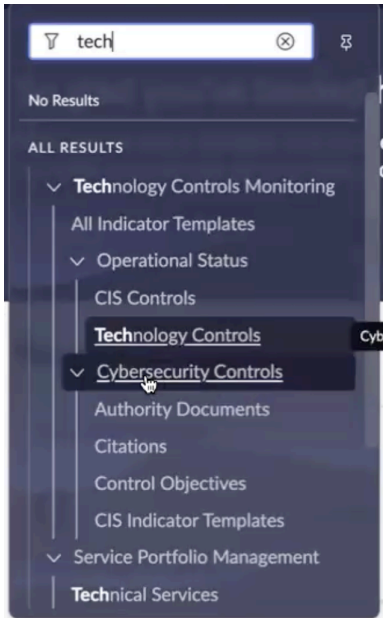
Beginning with the Utah release, Technology Controls Monitoring Accelerator provides pre-packaged CIS v8 controls and indicator templates.

#### Procedure

1. Navigate to **All** > **Technology Controls Monitoring** > **Operational Status**.

   You can view the module as shown in the example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




**Note:** The CIS controls module is renamed from CIS controls @R to Cybersecurity Controls. The Indicator Templates module is renamed to CIS Indicator Templates.

2. Select either **CIS Controls** or **Technology Controls**.

**Note:** The screen shown below results from selecting **CIS Controls**. The default columns will be slightly different if you select **Technology Controls**. However, you can select the gear icon to add or remove columns as needed.

**Indicator templates operational status**

Indicator templates operational status [CIS controls view] Search Control description Search 1 to 20 of 55

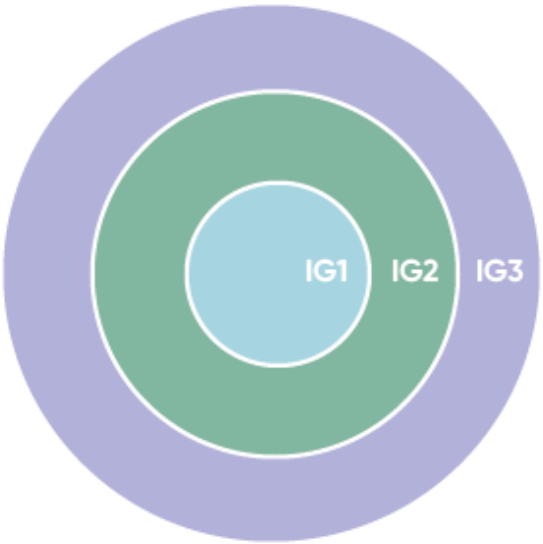
All > Control family starts with CIS > Indicator template type != Manual

| Controls | Control family | Control description ▲ | Domain | Implementation Group (IG) | Compliance validated by | Validating technology |
|---|---|---|---|---|---|---|
| CIS Control 6.2 | CIS Control 6 | Activate audit logging | Basic | IG1,IG2,IG3 | Configuration Compliance | false |
| CIS Control 2.6 | CIS Control 2 | Address unapproved software | Basic | IG1,IG2,IG3 | Software Asset Management Professional Core | false |
| CIS Control 1.6 | CIS Control 1 | Address Unauthorized Assets | Basic | IG1,IG2,IG3 | Security Incident Response | false |
| CIS Control 16.13 | CIS Control 16 | Alert on Account Login Behavior Deviation | Organizational | IG3 | Security Incident Response | false |
| CIS Control 19.2 | CIS Control 19 | Assign Job Titles and Duties for Inciden... | Organizational | IG2,IG3 | Incident Management | true |
| CIS Control 4.2 | CIS Control 4 | Change Default Passwords | Basic | IG1,IG2,IG3 | Configuration Compliance | false |
| CIS Control 3.6 | CIS Control 3 | Compare Back-to-back Vulnerability Scans | Basic | IG2,IG3 | Vulnerability Response | false |
| CIS Control 8.4 | CIS Control 8 | Configure Anti-Malware Scanning of Remov... | Foundational | IG1,IG2,IG3 | Configuration Compliance | false |
| CIS Control 8.5 | CIS Control 8 | Configure Devices Not To Auto-run Content | Foundational | IG1,IG2,IG3 | Configuration Compliance | false |
| CIS Control 19.8 | CIS Control 19 | Create Incident Scoring and Prioritizati... | Organizational | IG3 | Security Incident Response | false |

Each control includes the following information.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Operational Status

| Field | Description |
|---|---|
| Controls | The controls included when you download and activate the Cybersecurity Controls Accelerator application. |
| Control family and description | The family and description of the control as defined in the CIS Controls. |
| Domain | Domains of the controls:<br>◦ Basic<br>◦ Foundational<br>◦ Organizational |
| Implementation Group (IG) | The implementation group to which the control is included: IG1, IG2, or IG3. IG1 covers most of the essential security controls to serve as a foundation. Then, as needed to improve your security posture, you can add IG2 and IG3 to provide additional levels of support.<br>As illustrated here, IG2 includes all of the controls included in IG1, and IG3 includes all of the controls in IG1 and IG2.<br>  |
| Compliance validated by | The technology on your instance you can use to automate the validation of your controls. |
| Validating technology activated? | Identifies whether the specified technology is activated in your instance. |
| Controls implemented? | Identifies whether you have adopted the control objective and deployed it in your system. |
| Indicator template type | Identifies whether you have an indicator template type defined so you can begin validating and monitoring the control. The available types are Basic, Manual, and Script. |
| Source table | The source table for the data being monitored by the control. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### View the Cybersecurity Controls module

View the Cybersecurity Controls module for a list of the Authority documents, Controls, Control Objectives, and CIS Indicator Templates mapped to specific CIS controls classified by domain, implementation group, and ISO controls.

**Before you begin**

Role required: admin or sn_compliance.reader

**About this task**

**Note:** The Authority documents, Controls, and Control Objectives display the data related to source CIS, CIS v8, and CSA CCM v4. The module filters display the following data:

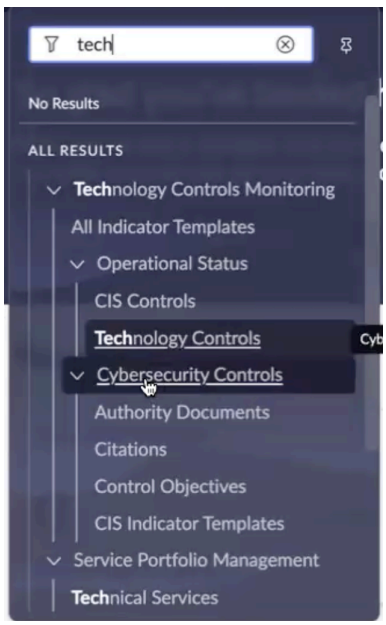
- Authority Document - Source is CIS or CIS v8 or CSA CCM v4.
- Citations - Source is CIS or CIS v8 or CSA CCM v4.
- Control objectives - Source is CIS or CIS v8 or CSA CCM v4.
- Indicator templates - Source is CIS or CIS v8.

Beginning with the Utah release, Technology Controls Monitoring Accelerator provides pre-packaged CIS v8 controls and indicator templates.

**Procedure**

1. Navigate to **All** > **Technology Controls Monitoring** > **Cybersecurity Controls**.

   You can view the module as shown in the example.




   **Note:** The CIS controls module is renamed from CIS controls @R to Cybersecurity Controls. The Indicator Templates module is renamed to CIS Indicator Templates.

2. Select **Authority Documents**.

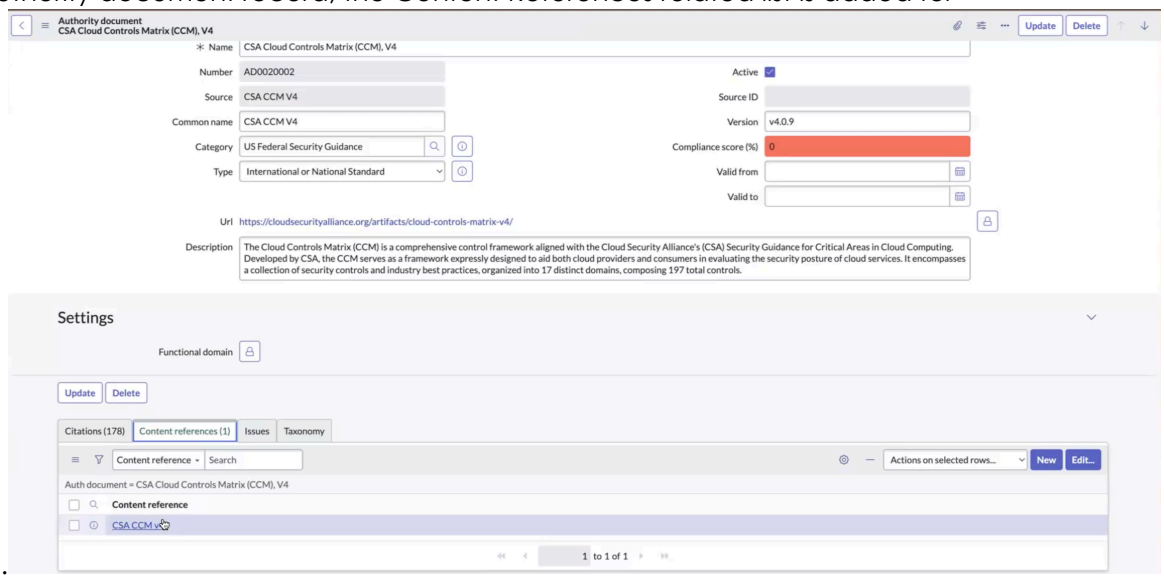
   The authority documents for source CIS, CIS v8, and CSA CCM v4 are listed as shown in the example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

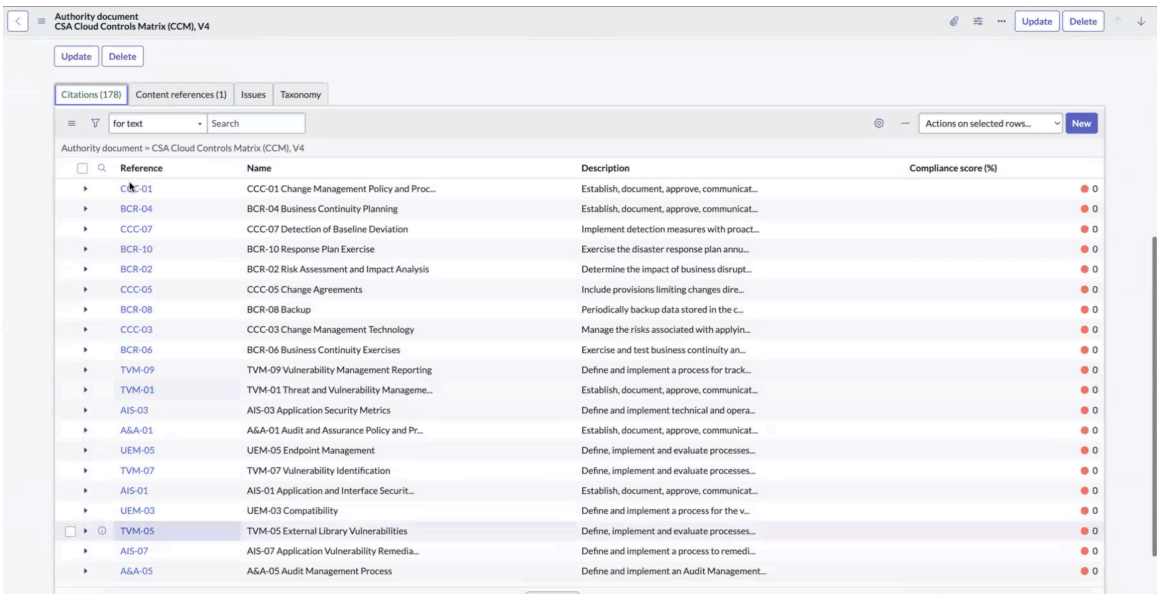



The authority document ADCIS10002 is added for CIS v8. Similarly, AD0020002 is added for CSACCMv4.

For the authority document record, the Content References related list is added for mapping.



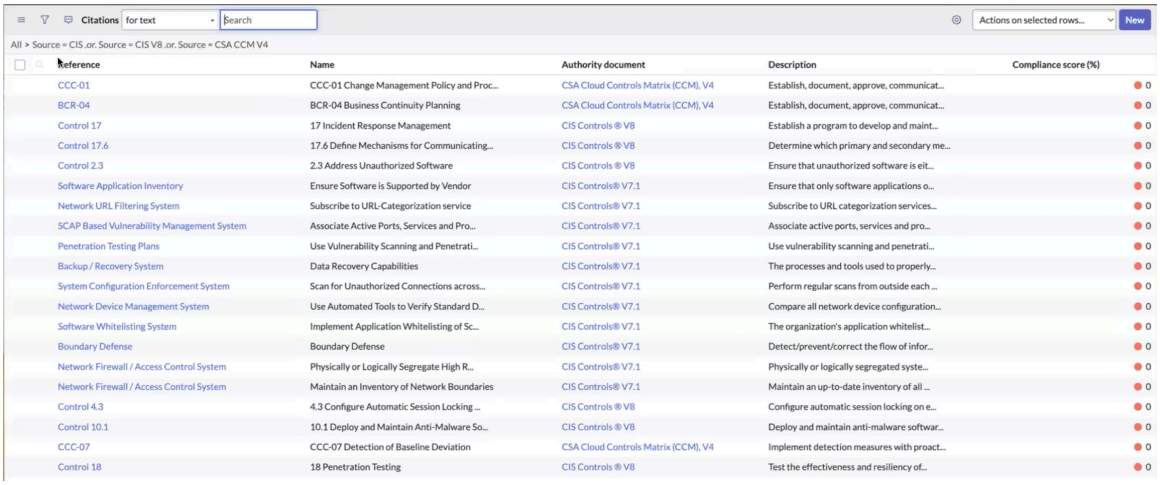

The citations associated with the authority document are shown in the example.



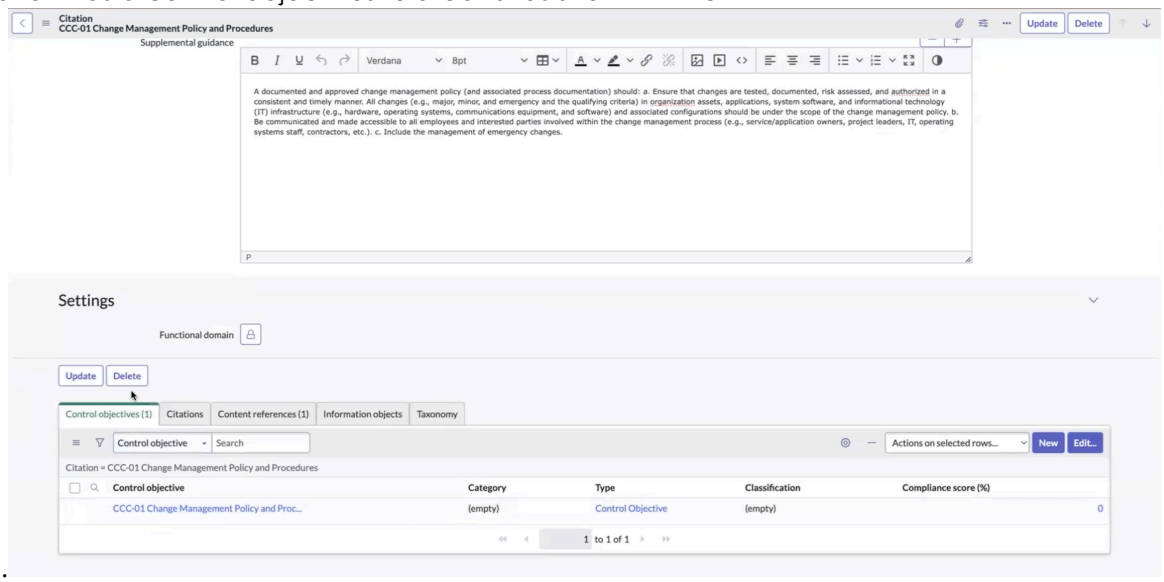

3. Select **Citations**.

The citations for source CIS, CIS v8, and CSA CCM v4 are listed as shown in the example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



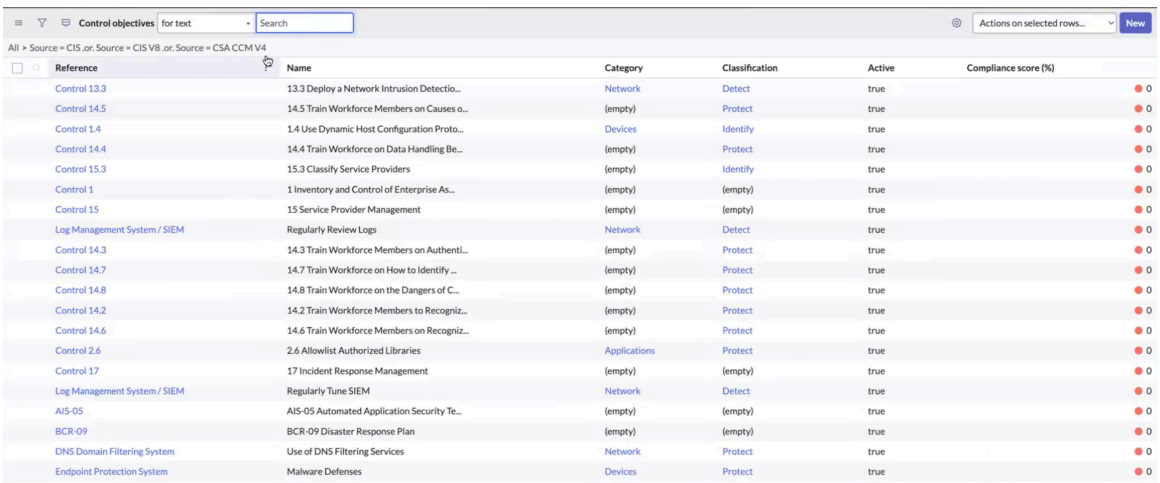

Every citation has a control objectives related list as shown in the




example.

4. Select **Control Objectives**.

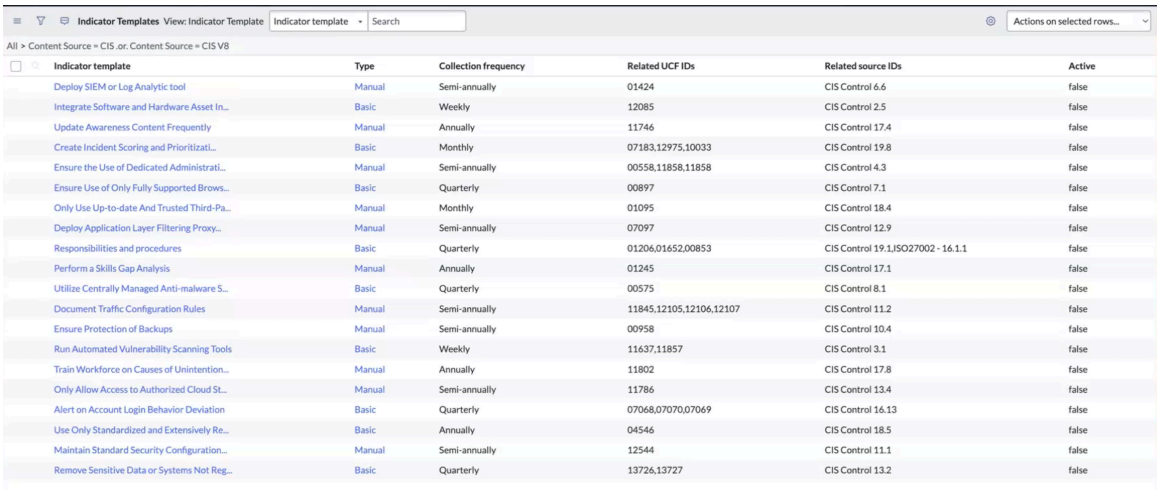
   The control objectives for source CIS, CIS v8, and CSA CCM v4 are listed as shown in the example.




5. Select **CIS Indicator Templates**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The CIS indicator templates for source CIS, CIS v8, and CSA CCM v4 are listed as shown in the example.

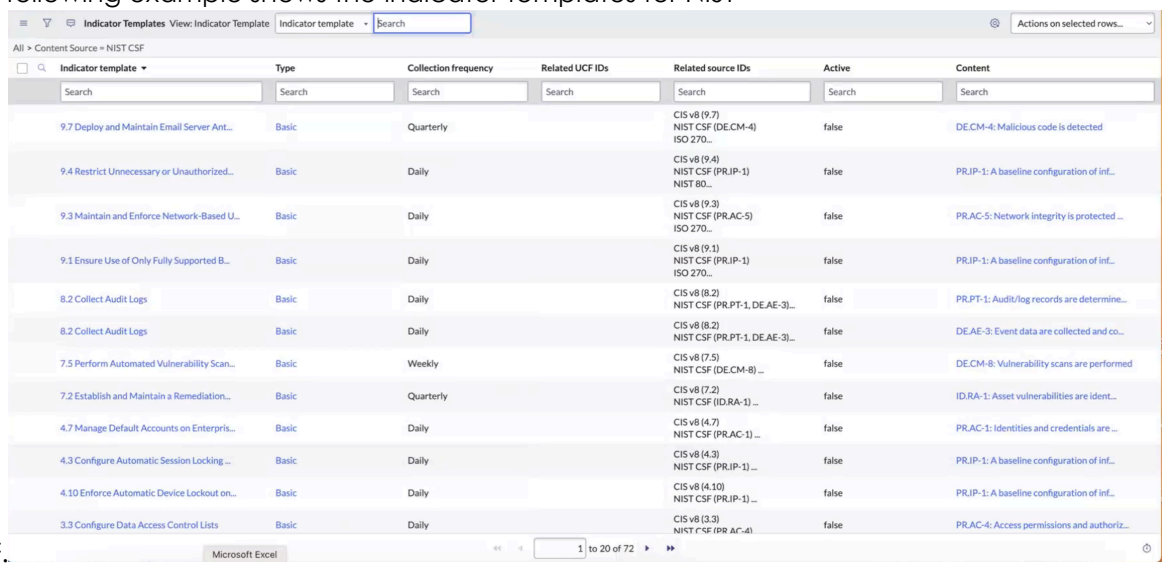


Indicator Templates View: Indicator Template | Indicator template | Search | Actions on selected rows...

All > Content Source = CIS .or. Content Source = CIS V8

| Indicator template | Type | Collection frequency | Related UCF IDs | Related source IDs | Active |
|---|---|---|---|---|---|
| Deploy SIEM or Log Analytic tool | Manual | Semi-annually | 01424 | CIS Control 6.6 | false |
| Integrate Software and Hardware Asset In... | Basic | Weekly | 12085 | CIS Control 2.5 | false |
| Update Awareness Content Frequently | Manual | Annually | 11746 | CIS Control 17.4 | false |
| Create Incident Scoring and Prioritizati... | Basic | Monthly | 07183,12975,10033 | CIS Control 19.8 | false |
| Ensure the Use of Dedicated Administrati... | Manual | Semi-annually | 00558,11858,11858 | CIS Control 4.3 | false |
| Ensure Use of Only Fully Supported Brows... | Basic | Quarterly | 00897 | CIS Control 7.1 | false |
| Only Use Up-to-date And Trusted Third-Pa... | Manual | Monthly | 01095 | CIS Control 18.4 | false |
| Deploy Application Layer Filtering Proxy... | Manual | Semi-annually | 07097 | CIS Control 12.9 | false |
| Responsibilities and procedures | Basic | Quarterly | 01206,01652,00853 | CIS Control 19.1,ISO27002 - 16.1.1 | false |
| Perform a Skills Gap Analysis | Manual | Annually | 01245 | CIS Control 17.1 | false |
| Utilize Centrally Managed Anti-malware S... | Basic | Quarterly | 00575 | CIS Control 8.1 | false |
| Document Traffic Configuration Rules | Manual | Semi-annually | 11845,12105,12106,12107 | CIS Control 11.2 | false |
| Ensure Protection of Backups | Manual | Semi-annually | 00958 | CIS Control 10.4 | false |
| Run Automated Vulnerability Scanning Tools | Basic | Weekly | 11637,11857 | CIS Control 3.1 | false |
| Train Workforce on Causes of Unintention... | Manual | Annually | 11802 | CIS Control 17.8 | false |
| Only Allow Access to Authorized Cloud St... | Manual | Semi-annually | 11786 | CIS Control 13.4 | false |
| Alert on Account Login Behavior Deviation | Basic | Quarterly | 07068,07070,07069 | CIS Control 16.13 | false |
| Use Only Standardized and Extensively Re... | Basic | Annually | 04546 | CIS Control 18.5 | false |
| Maintain Standard Security Configuration... | Manual | Semi-annually | 12544 | CIS Control 11.1 | false |
| Remove Sensitive Data or Systems Not Reg... | Basic | Quarterly | 13726,13727 | CIS Control 13.2 | false |

You can view the indicator templates for different sources. The following example shows the indicator templates for NIST CSF.



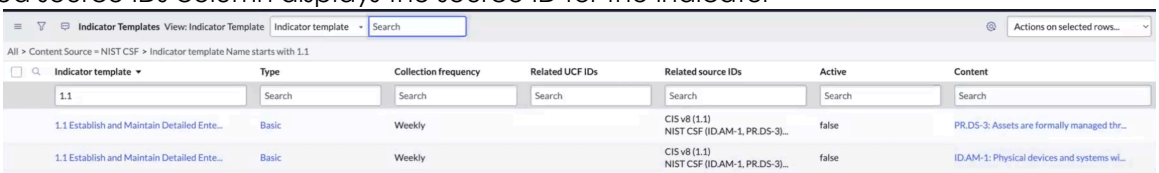
Indicator Templates View: Indicator Template | Indicator template | Search | Actions on selected rows...

All > Content Source = NIST CSF

| Indicator template | Type | Collection frequency | Related UCF IDs | Related source IDs | Active | Content |
|---|---|---|---|---|---|---|
| 9.7 Deploy and Maintain Email Server Ant... | Basic | Quarterly | | CIS v8 (9.7) NIST CSF (DE.CM-4) ISO 270... | false | DE.CM-4: Malicious code is detected |
| 9.4 Restrict Unnecessary or Unauthorized... | Basic | Daily | | CIS v8 (9.4) NIST CSF (PR.IP-1) NIST 80... | false | PR.IP-1: A baseline configuration of inf... |
| 9.3 Maintain and Enforce Network-Based U... | Basic | Daily | | CIS v8 (9.3) NIST CSF (PR.AC-5) ISO 270... | false | PR.AC-5: Network integrity is protected ... |
| 9.1 Ensure Use of Only Fully Supported B... | Basic | Daily | | CIS v8 (9.1) NIST CSF (PR.IP-1) ISO 270... | false | PR.IP-1: A baseline configuration of inf... |
| 8.2 Collect Audit Logs | Basic | Daily | | CIS v8 (8.2) NIST CSF (PR.PT-1, DE.AE-3)... | false | PR.PT-1: Audit/log records are determine... |
| 8.2 Collect Audit Logs | Basic | Daily | | CIS v8 (8.2) NIST CSF (PR.PT-1, DE.AE-3)... | false | DE.AE-3: Event data are collected and co... |
| 7.5 Perform Automated Vulnerability Scan... | Basic | Weekly | | CIS v8 (7.5) NIST CSF (DE.CM-8) ... | false | DE.CM-8: Vulnerability scans are performed |
| 7.2 Establish and Maintain a Remediation... | Basic | Quarterly | | CIS v8 (7.2) NIST CSF (ID.RA-1) ... | false | ID.RA-1: Asset vulnerabilities are ident... |
| 4.7 Manage Default Accounts on Enterpris... | Basic | Daily | | CIS v8 (4.7) NIST CSF (PR.AC-1) ... | false | PR.AC-1: Identities and credentials are ... |
| 4.3 Configure Automatic Session Locking ... | Basic | Daily | | CIS v8 (4.3) NIST CSF (PR.IP-1) ... | false | PR.IP-1: A baseline configuration of inf... |
| 4.10 Enforce Automatic Device Lockout on... | Basic | Daily | | CIS v8 (4.10) NIST CSF (PR.IP-1) ... | false | PR.IP-1: A baseline configuration of inf... |
| 3.3 Configure Data Access Control Lists | Basic | Daily | | CIS v8 (3.3) NIST CSF (PR.AC-4) | false | PR.AC-4: Access permissions and authoriz... |

Microsoft Excel | 1 to 20 of 72

The Related source IDs column displays the source ID for the indicator template.



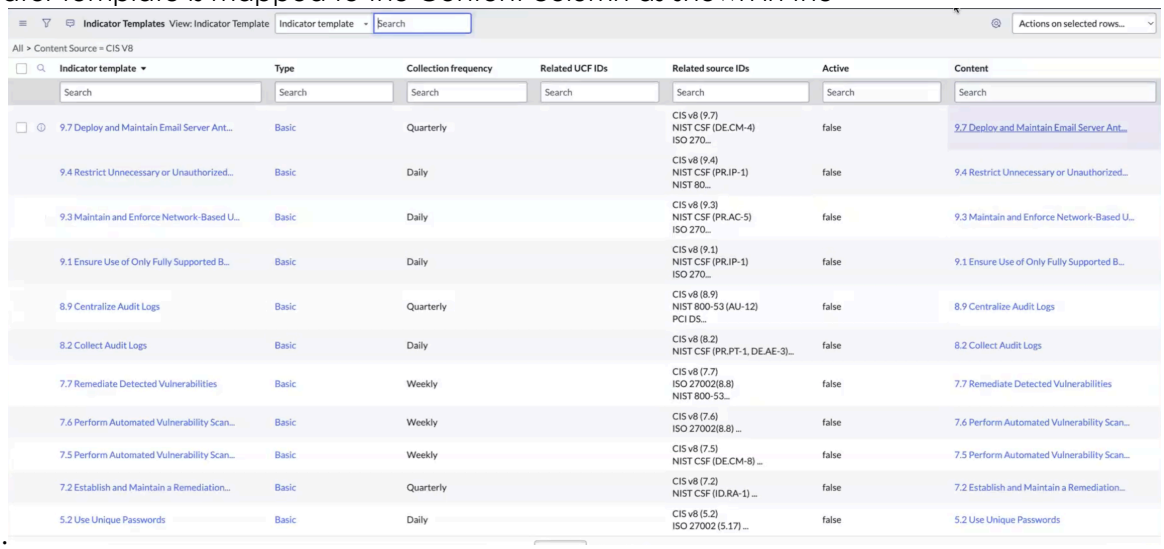
Indicator Templates View: Indicator Template | Indicator template | Search | Actions on selected rows...

All > Content Source = NIST CSF > Indicator template Name starts with 1.1

| Indicator template | Type | Collection frequency | Related UCF IDs | Related source IDs | Active | Content |
|---|---|---|---|---|---|---|
| 1.1 | | | | | | |
| 1.1 Establish and Maintain Detailed Ente... | Basic | Weekly | | CIS v8 (1.1) NIST CSF (ID.AM-1, PR.DS-3)... | false | PR.DS-3: Assets are formally managed thr... |
| 1.1 Establish and Maintain Detailed Ente... | Basic | Weekly | | CIS v8 (1.1) NIST CSF (ID.AM-1, PR.DS-3)... | false | ID.AM-1: Physical devices and systems wi... |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The indicator template is mapped to the Content column as shown in the example.




6. Select **CIS Indicator Templates**.
   The CIS Indicator Templates are displayed in the instance.

### Using indicator templates

Indicators collect data to monitor a single control or risk. Indicator templates allow you to create multiple indicators for similar controls or risks. The Technology Controls Monitoring Accelerator application provides a collection of 171 predefined indicator templates for monitoring cybersecurity controls.

## Indicators and Indicator templates

The indicators collect data to monitor the controls and risks and collect the audit evidence. Indicators monitor a single control or risk.

The indicator templates allow the creation of multiple indicators for similar controls or risks.

The indicator templates obtained with the Technology Controls Monitoring Accelerator application provide the instructions that you must run the indicators, as described in the following sections.

Supporting information can be collected for the indicators through automatic data collection or manual tasks. Indicator results are then used to perform the following tasks:

- Create issues for the controls.
- Update the risk scores.
- Provide supporting information for the audit activities and control testing

The following types of indicators are available:

1. Basic: Evidence is collected from on the source table.
2. Manual: Evidence is not collected. This type of indicator requires a third party data source.
3. Scripted: Evidence can be collected from multiple source tables.

## Flow of the indicator process

The indicator process consists of the following steps:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Set up the indicator template.
- Apply the indicator template to a risk statement or control. When the control or risk statement is scoped with an entity type or specific entities, then all the controls or risks under that control objective or risk statement have an indicator generated for them.

Indicators can be automated or manual. The indicator tasks are generated that show the final state of the indicator.

## Examples of automated indicators and manual indicators

An example of an automated indicator would be to check that all servers in the CMDB are up to date. Another example would be that all LDAP passwords are less than three months old.

An example of a manual indicator would be to ask the network administrator to conduct the annual Network Penetration Tests are conducted and the results are attached to the task. If a result indicates failed or not passed, it is used to trigger the creation of GRC issues.

## Usage of indicator templates

You can link the indicator templates to the policy statements or risk statements so that the indicators are automatically created for the controls or risks. The status of the controls is also automatically calculated by the linked indicator results and it may affect any linked risks. For example, if the indicator tied to a control fails, then the overall status cannot be completed unless the remediation task is closed by the user.

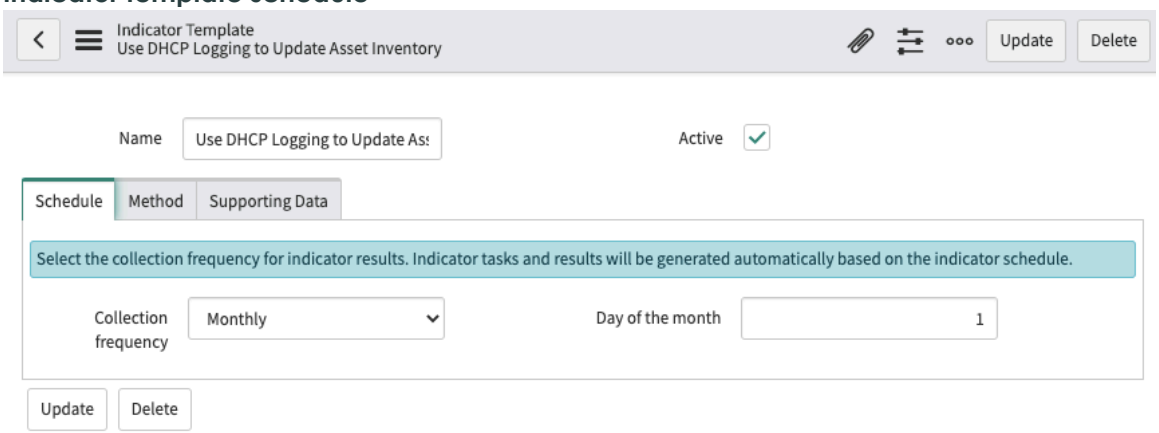
The Calculated Risk Score for the risk is also adjusted automatically by the indicators results of the risk. The Indicator Failure Factor field in the Risk table displays the impact of the failures.

**Note:** Indicators are not weighted. When you weigh their impact on a control or risk, they are considered equalizing. Indicators are not executed when the risks and controls are in the **Retired** state.

## Indicator template collection frequency

Each indicator template includes a schedule for identifying the frequency of data collection, as shown here.

**Indicator template schedule**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

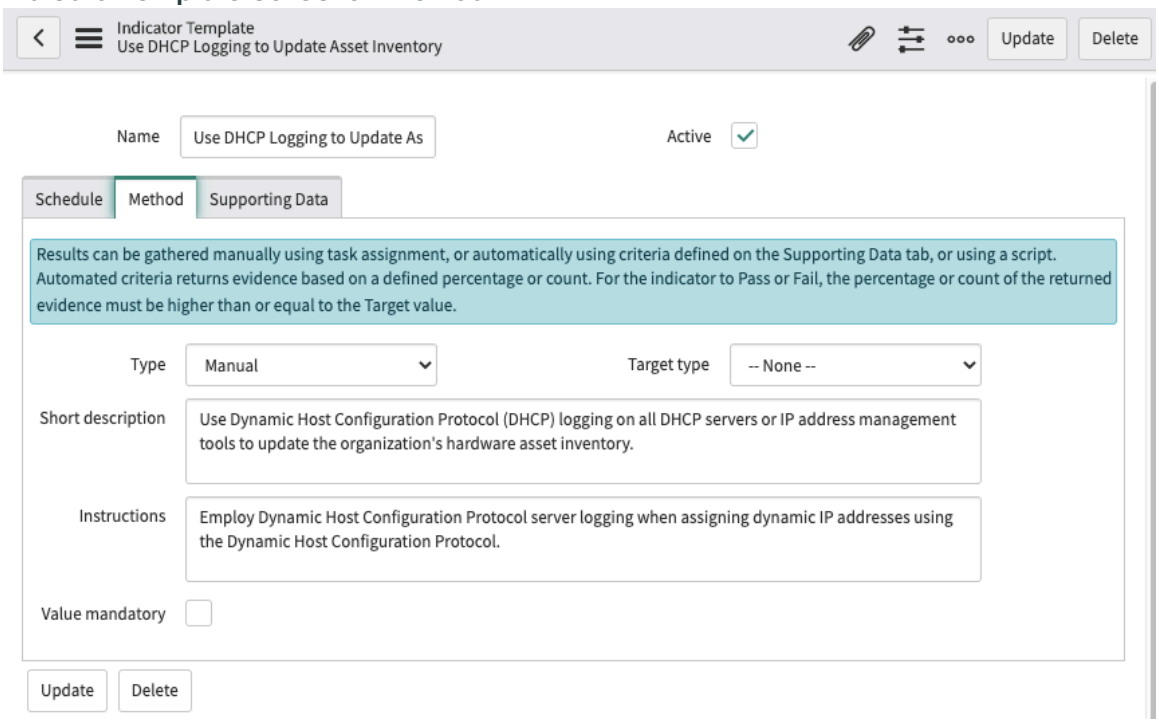
### Schedule tab

| Field | Description |
|---|---|
| Collection frequency | Collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule.<br>• Daily<br>• Weekly: The day of the week to perform the collection.<br>• Monthly: The day of the month to perform the collection.<br>• Quarterly: The date of the first collection run.<br>• Semi-Annually: The date of the first collection run.<br>• Annually: The month and day to perform the collection. |

## Indicator template collection method

The Method tab identifies how the results are collected, as shown here.

### Indicator template collection method




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Method tab

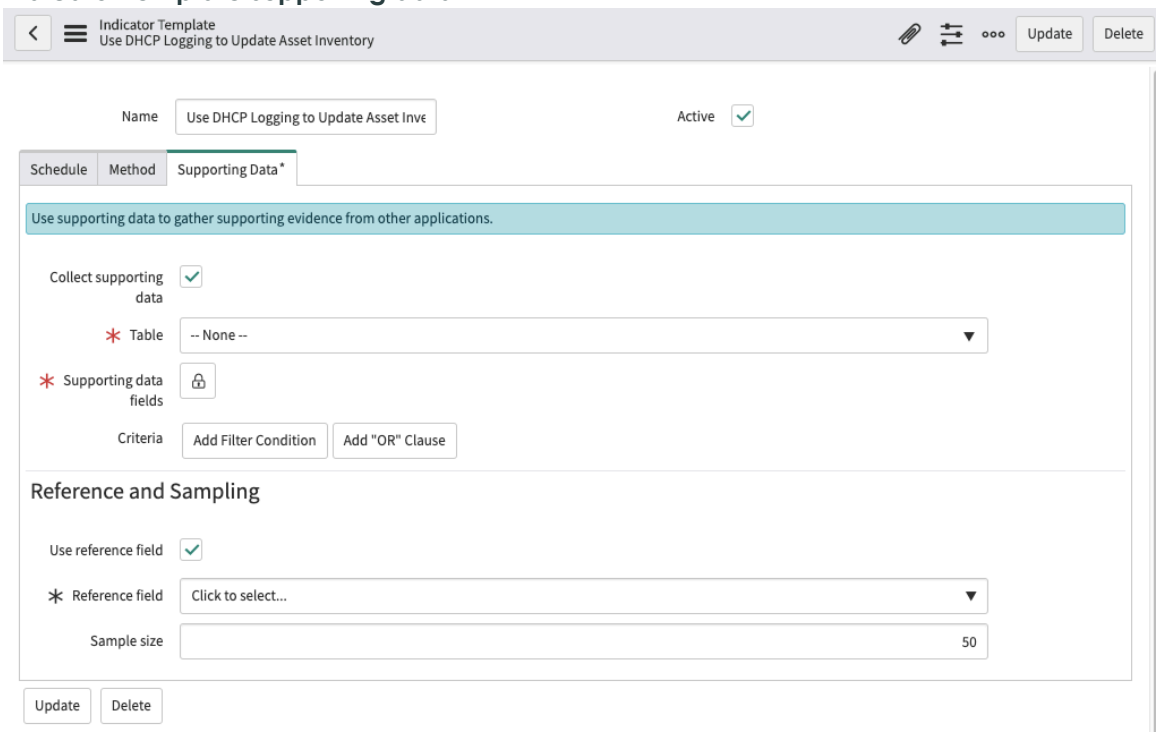
| Field | Description |
|---|---|
| Type | Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script. |
| Target Type | Identifies whether the target is a percentage or a count. |
| Short Description | If **Type = Manual**, a brief description of the issue. |
| Instructions | If **Type = Manual**, instructions for the collection of indicator results. |
| Value Mandatory | If **Type = Manual**, the check box indicates whether the value is mandatory for the indicator task. |
| Passed/Failed | If **Type = Basic**, the conditions defined on the Supporting Data tab are met, and the results exceed the **Target** value, it indicates whether the indicator passed or failed. |
| Target | If **Type = Basic**, the threshold by which the results returned based on the conditions defined on the Supporting Data tab determine whether the indicator template passes or fails. |
| PA Threshold | If **Type = PA Indicator**, the associated PA Threshold. |
| Script | If **Type = Script**, the script that obtains the desired system information. |

## Indicator template supporting data

Starting with version 10.1, the Supporting Data tab displays actual historical data for the supporting data records from the indicator results or indicator tasks. In earlier versions, only the real-time state of the records collected could be viewed.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator template supporting data




### Indicator template supporting data

| Field | Description |
|---|---|
| Collect supporting data | Indicates that you want to collect supporting data. The following three fields are displayed. |
| Table | The supporting data table. |
| Supporting Data Fields | The fields from the supporting data table to be considered. |
| Criteria | Filter conditions. |
| Use reference field | Indicates that you want to use a reference field. The following two fields are displayed. |
| Reference field | The reference field that you want to use for sampling. |
| Sample size | The number of records you want to use for data sampling. |

You can also view information on the following tabs:

- Indicators
- Control Objectives/Risk Statements
- Content References

**Note:** The **Control Objectives/Risk Statements** tab allows you to reuse the same template for multiple control objectives or risk statements.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for controls

The Technology Controls Monitoring Accelerator includes 273 indicator templates (94 Basic, 174 Manual, and 5 Scripted) for CIS v7 and includes new 67 indicator templates (64 Basic and 3 Scripted) for CIS v8.

When the Technology Controls Monitoring Accelerator is used along with the Cybersecurity Controls Accelerator application, you can manage indicator templates within the Cybersecurity Controls Accelerator application.

When Technology Controls Monitoring Accelerator is run as a standalone application; however, it can be run with the Policy and Compliance Management application. You can also map UCF controls to indicator templates from with the Policy and Compliance Management application.

**Note:** For information on the different types of indicator templates, see Using indicator templates.

## Indicator templates for CIS v8 Controls

The following table lists the indicator templates for CIS v8 Controls.

**Note:** Controls currently not covered by either basic or scripted indicator templates have manual indicator templates defined for the purposes of compliance validation. For more information on CIS v8 indicator templates, see KB0555526.

### Indicator templates for CIS v8 Controls

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| CIS Control V8 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory:<br><br>Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud | BASIC | HAM | cmdb_ci_hardware | CIS v8 (1.1) CSF (ID.AM-1, PR.DS-3) ISO 27002 (5.9, 8.8) PCI (9.5.1, 9.5.1.1, 11.2, 11.2.1, 11.2.2, 12.5, 12.5.1) CCM (UEM-04) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently. | | | | |
| CIS Control V8 1.2 | Address Unauthorized Assets:<br><br>Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset. | BASIC | CMDB | cmdb_ci | CIS v8 (1.2) NIST (CM-8) PCI (11.2.1) |
| CIS Control V8 1.3 | Utilize an Active Discovery Tool:<br><br>Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently. | BASIC | Discovery | cmdb_discovery | CIS v8 (1.3) CSF (DE.CM-7) NIST (CM-8(1)) CCM (UEM-05) |
| CIS Control V8 1.4 | Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory:<br><br>Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently. | Manual | NA | NA | |
| CIS Control V8 1.5 | Use a Passive Asset Discovery Tool:<br><br>Use a passive discovery tool to identify assets connected to the | BASIC | Discovery | discovery_network_track | CIS v8 (1.5) CSF (DE.CM-7) NIST (CM-8(3)) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently. | | | | |
| CIS Control V8 2.1 | Establish and Maintain a Software Inventory:<br><br>Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently. | BASIC | SAM | cmdb_ci_application_software | CIS v8 (2.1) CSF (ID.AM-2) ISO (5.9) NIST (SI-4) PCI (1.2.5, 6.3.2) CCM (UEM-02) |
| CIS Control V8 2.2 | Ensure Authorized Software is Currently Supported<br><br>Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently. | Manual | NA | NA | |
| CIS Control V8 2.3 | Address Unauthorized Software:<br><br>Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented | SCRIPTED | SAM | cmdb_sam_sw_install | CIS v8 (2.3) CSF (DE.CM-7) ISO (8.7) NIST (CM-8(3)) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | exception. Review monthly, or more frequently. | | | | PCI (12.3.4) |
| CIS Control V8 2.4 | Utilize Automated Software Inventory Tools:<br><br>Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software. | BASIC | SAM | cmdb_ci_application_software | CIS v8 (2.4) CSF (DE.CM-7) NIST (SI-4) |
| CIS Control V8 2.5 | Allowlist Authorized Software:<br><br>Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently. | SCRIPTED | SAM | cmdb_sam_sw_install | CIS v8 (2.5) CSF (DE.CM-7) ISO (8.7, 8.17) PCI (1.2.5, 2.2.4) |
| CIS Control V8 2.6 | Allowlist Authorized Libraries:<br><br>Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently. | BASIC | VR | sn_vulc_result | CIS v8 (2.6) CSF (DE.CM-7) ISO (8.19) PCI (1.2.5, 2.2.4) |
| CIS Control V8 2.7 | Allowlist Authorized Scripts:<br><br>Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently. | BASIC | VR | sn_vulc_result | CIS v8 (2.7) CSF (PR.IP-1, PR.PT-3) NIST (CM-8) PCI (1.2.5, 2.2.4, 6.4.3) |
| CIS Control V8 3.1 | Establish and Maintain a Data Management Process: | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | | | | |
| CIS Control V8 3.10 | Encrypt Sensitive Data in Transit:<br><br>Encrypt sensitive data in transit. Example implementations can include, Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | BASIC | Discovery | sn_disco_cert_mgmt_cmdb_installed_c | CIS v8 (3.10) CSF (PR.IP-6, PR.DS-2) ISO (5.1, 5.9, 8.1, 5.14) NIST (CM-7(1), CM-10) PCI (9.4, 9.4.2, 2.2.7, 4.1.1, 4.2.1, 4.2.1.2, 4.2.2, 8.3.2) CCM (DSP-01, DSP-06, GRC-03, CEK-03) |
| CIS Control V8 3.11 | Encrypt Sensitive Data At Rest:<br><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does | BASIC | CMDB | cmdb_rel_c | CIS v8 (3.11) CSF (PR.DS-1) ISO (5.33) NIST (CM-7) PCI (3.1.1, 3.3.2, 3.3.3, 3.5.1, 3.5.1.2, 3.5.1.3, 8.3.2) CCM |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | not permit access to the plain-text data. | | | | (DSP-10, CEK-03) |
| CIS Control V8 3.12 | Segment Data Processing and Storage Based on Sensitivity:<br><br>Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data. | Manual | NA | NA | |
| CIS Control V8 3.13 | Deploy a Data Loss Prevention Solution:<br><br>Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory. | BASIC | CMDB | cmdb_rel_ci | CIS v8 (3.13) CSF (PR.DS-5) ISO (5.13, 8.12) NIST (CM-7) CCM (DSP-10, UEM-11) |
| CIS Control V8 3.14 | Log Sensitive Data Access:<br><br>Log sensitive data access, including modification and disposal. | BASIC | VR | sn_vulc_result | CIS v8 (3.14) ISO (-8.15) NIST (CM-7(1)) PCI (10.2.1, 10.2.1.1) CCM (DSP-17, IAM-12, LOG-04) |
| CIS Control V8 3.2 | Establish and Maintain a Data Inventory:<br><br>Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | a minimum, with a priority on sensitive data. | | | | |
| CIS Control V8 3.3 | Configure Data Access Control Lists:<br><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | BASIC | VR | sn_vulc_result | CIS v8 (3.3) CSF (PR.AC-4) ISO (5.1, 5.15, 8.3, 8.4) NIST (SA-22) PCI (1.3.1, 7.1) CCM (DSP-17, IAM-05) |
| CIS Control V8 3.4 | Enforce Data Retention:<br><br>Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines. | Manual | NA | NA | |
| CIS Control V8 3.5 | Securely Dispose of Data:<br><br>Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity. | Manual | NA | NA | |
| CIS Control V8 3.6 | Encrypt Data on End-User Devices:<br><br>Encrypt data on end-user devices containing sensitive data. Example implementations can include Windows BitLocker™, Apple FileVault™, Linux dm-crypt™. | BASIC | CMDB | cmdb_rel_ci | CIS v8 (3.6) ISO (6.7, 7.1, 8.1) NIST (CM-100) CCM (CEK-03, UEM-08) |
| CIS Control V8 3.7 | Establish and Maintain a Data Classification Scheme:<br><br>Establish and maintain an overall data classification scheme for the enterprise. Enterprises may | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard. | | | | |
| CIS Control V8 3.8 | Document Data Flows:<br><br>Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Manual | NA | NA | |
| CIS Control V8 3.9 | Encrypt Data on Removable Media:<br><br>Encrypt data on removable media. | Manual | NA | NA | |
| CIS Control V8 4.1 | Establish and Maintain a Secure Configuration Process:<br><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/ IoT devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Manual | NA | NA | |
| CIS Control V8 4.10 | Enforce Automatic Device Lockout on Portable End-User Devices: | BASIC | VR | sn_vulc_result | CIS v8 (4.10) CSF (PR.IP-1) ISO (8.1, 8.5, 8.9) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft InTune Device Lock and Apple Configuration Profile maxFailedAttempts. | | | | NIST (SI-7, PM-5(1)) PCI (1.1.1, 1.2.1, 1.2.6, 1.5.1, 1.2.7, 2.1.1, 2.2.1, 8.3.4) CCM (CCC-01, GRC-03, IVS-04) |
| CIS Control V8 4.11 | Enforce Remote Wipe Capability on Portable End-User Devices:<br><br>Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise. | Manual | NA | NA | |
| CIS Control V8 4.12 | Separate Enterprise Workspaces on Mobile End-User Devices:<br><br>Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple Configuration Profile or Android Work Profile to separate enterprise applications and data from personal applications and data. | Manual | NA | NA | |
| CIS Control V8 4.2 | Establish and Maintain a Secure Configuration Process for Network Infrastructure:<br><br>Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | enterprise changes occur that could impact this Safeguard. | | | | |
| CIS Control V8 4.3 | Configure Automatic Session Locking on Enterprise Assets:<br><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. | BASIC | VR | sn_vulc_result | CIS v8 (4.3) CSF (PR.IP-1) ISO (8.5, 8.9) PCI (8.2.8) CCM (UEM-06) |
| CIS Control V8 4.4 | Implement and Manage a Firewall on Servers:<br><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent. | BASIC | VR | sn_vulc_result | CIS v8 (4.4) PCI (1.2.1, 1.4.1) |
| CIS Control V8 4.5 | Implement and Manage a Firewall on End-User Devices:<br><br>Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. | Manual | NA | NA | |
| CIS Control V8 4.6 | Securely Manage Enterprise Assets and Software:<br><br>Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. | | | | |
| CIS Control V8 4.7 | Manage Default Accounts on Enterprise Assets and Software:<br><br>Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable. | BASIC | VR | sn_vulc_result | CIS v8 (4.7) CSF (PR.AC-1) ISO (8.2, 8.9) NIST (SI-12) PCI (2.2.2, 2.3.1) |
| CIS Control V8 4.8 | Uninstall or Disable Unnecessary Services on Enterprise Assets and Software:<br><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | Manual | NA | NA | |
| CIS Control V8 4.9 | Configure Trusted DNS Servers on Enterprise Assets:<br><br>Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers. | BASIC | VR | sn_vulc_result | CIS v8 (4.9) NIST (PM-5(1)) |
| CIS Control V8 5.1 | Establish and Maintain an Inventory of Accounts:<br><br>Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. | | | | |
| CIS Control V8 5.2 | Use Unique Passwords:<br><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. | BASIC | VR | sn_vulc_result | CIS v8 (5.2) ISO (5.17) NIST (AC-5) PCI (2.2.2, 8.3.5, 8.5.6, 8.6.3) CCM (IAM-02) |
| CIS Control V8 5.3 | Disable Dormant Accounts:<br><br>Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported. | Manual | NA | NA | |
| CIS Control V8 5.4 | Restrict Administrator Privileges to Dedicated Administrator Accounts:<br><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. | Manual | NA | NA | |
| CIS Control V8 5.5 | Establish and Maintain an Inventory of Service Accounts:<br><br>Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | reviews to validate all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. | | | | |
| CIS Control V8 5.6 | Centralize Account Management:<br><br>Centralize account management through a directory or identity service. | Manual | NA | NA | |
| CIS Control V8 6.1 | Establish an Access Granting Process:<br><br>Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. | Manual | NA | NA | |
| CIS Control V8 6.2 | Establish an Access Revoking Process:<br><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. | Manual | NA | NA | |
| CIS Control V8 6.3 | Require MFA for Externally-Exposed Applications:<br><br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| CIS Control V8 6.4 | Require MFA for Remote Network Access:<br><br>Require MFA for remote network access. | Manual | NA | NA | |
| CIS Control V8 6.5 | Require MFA for Administrative Access:<br><br>Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider. | Manual | NA | NA | |
| CIS Control V8 6.6 | Establish and Maintain an Inventory of Authentication and Authorization Systems:<br><br>Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently. | Manual | NA | NA | |
| CIS Control V8 6.7 | Centralize Access Control:<br><br>Centralize access control for all enterprise assets through a directory service or SSO provider, where supported. | Manual | NA | NA | |
| CIS Control V8 6.8 | Define and Maintain Role-Based Access Control:<br><br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | schedule at a minimum annually, or more frequently. | | | | |
| CIS Control V8 7.1 | Establish and Maintain a Vulnerability Management Process:<br><br>Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Manual | NA | NA | |
| CIS Control V8 7.2 | Establish and Maintain a Remediation Process:<br><br>Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews. | BASIC | VR | sn_vul_m2m_cis_v8 | CIS v8 (7.2) CSF (ID.RA-1) ISO (8.8) NIST (IA-5) PCI (6.3.1, 6.4.1) CCM (A&A-03, TVM-08, TVM-10) |
| CIS Control V8 7.3 | Perform Automated Operating System Patch Management:<br><br>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. | Manual | NA | NA | |
| CIS Control V8 7.4 | Perform Automated Application Patch Management:<br><br>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. | Manual | NA | NA | |
| CIS Control V8 7.5 | Perform Automated Vulnerability Scans of Internal Enterprise Assets: | BASIC | VR | sn_vul_ds_import_q_entry | CIS v8 (7.5) CSF (DE.CM-8) ISO (8.8) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool. | | | | NIST (SC-8(1)) PCI (11.3.1, 11.3.1.1, 11.3.1.2, 11.3.1.3) CCM (TVM-07) |
| CIS Control V8 7.6 | Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:<br><br>Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis. | BASIC | VR | sn_vul_ds_import_q_entry | |
| CIS Control V8 7.7 | Remediate Detected Vulnerabilities:<br><br>Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process. | BASIC | VR | sn_vul_app_vulnerability | CIS v8 (7.7) ISO (8.8) NIST (SC-28) PCI (11.3.1, 11.3.2, 11.3.2.1) CCM (TVM-03) |
| CIS Control V8 8.1 | Establish and Maintain an Audit Log Management Process:<br><br>Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Manual | NA | NA | |
| CIS Control V8 8.1 | Retain Audit Logs: | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | Retain audit logs across enterprise assets for a minimum of 90 days. | | | | |
| CIS Control V8 8.11 | Conduct Audit Log Reviews:<br><br>Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis. | Manual | NA | NA | |
| CIS Control V8 8.12 | Collect Service Provider Logs:<br><br>Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events. | Manual | NA | NA | |
| CIS Control V8 8.2 | Collect Audit Logs:<br><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. | BASIC | VR | sn_vulc_result | CIS v8 (8.2) CSF (PR.PT-1, DE.AE-3) ISO (8.15, 8.2) PCI (5.3.4, 6.4.1, 6.4.2, 10.2.1, 10.2.1.1, 10.2.1.2, 10.2.1.3, 10.2.1.4, 10.2.1.5, 10.2.1.6, 10.2.1.7, 10.2.2) CCM (LOG-08) |
| CIS Control V8 8.3 | Ensure Adequate Audit Log Storage:<br><br>Ensure that logging destinations maintain adequate storage to | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | comply with the enterprise's audit log management process. | | | | |
| CIS Control V8 8.4 | Standardize Time Synchronization:<br><br>Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported. | Manual | NA | NA | |
| CIS Control V8 8.5 | Collect Detailed Audit Logs:<br><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. | Manual | NA | NA | |
| CIS Control V8 8.6 | Collect DNS Query Audit Logs:<br><br>Collect DNS query audit logs on enterprise assets, where appropriate and supported. | Manual | NA | NA | |
| CIS Control V8 8.7 | Collect URL Request Audit Logs:<br><br>Collect URL request audit logs on enterprise assets, where appropriate and supported. | Manual | NA | NA | |
| CIS Control V8 8.8 | Collect Command-Line Audit Logs:<br><br>Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell™, BASH™, and remote administrative terminals. | Manual | NA | NA | |
| CIS Control V8 8.9 | Centralize Audit Logs: | BASIC | CMDB | cmdb_ci | CIS v8 (8.9) NIST (AU-12) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | Centralize, to the extent possible, audit log collection and retention across enterprise assets. | | | | PCI (10.3.3) |
| CIS Control V8 9.1 | Ensure Use of Only Fully Supported Browsers and Email Clients:<br><br>Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor. | BASIC | VR | sn_vulc_result | CIS v8 (9.1) CSF (PR.IP-1) ISO (8.1) NIST (CM-2) |
| CIS Control V8 9.2 | Use DNS Filtering Services:<br><br>Use DNS filtering services on all enterprise assets to block access to known malicious domains. | Manual | NA | NA | |
| CIS Control V8 9.3 | Maintain and Enforce Network-Based URL Filters:<br><br>Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets. | BASIC | VR | sn_vulc_result | CIS v8 (9.3) CSF (PR.AC-5) ISO (8.7, 8.23) NIST (CM-7) PCI (1.2.6, 1.4.2) |
| CIS Control V8 9.4 | Restrict Unnecessary or Unauthorized Browser and Email Client Extensions:<br><br>Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications. | BASIC | VR | sn_vulc_result | CIS v8 (9.4) CSF (PR.IP-1) NIST (CM-7(1)) PCI (2.2.4) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| CIS Control V8 9.5 | Implement DMARC:<br><br>To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards. | Manual | NA | NA | |
| CIS Control V8 9.6 | Block Unnecessary File Types:<br><br>Block unnecessary file types attempting to enter the enterprise's email gateway. | Manual | NA | NA | |
| CIS Control V8 9.7 | Deploy and Maintain Email Server Anti-Malware Protections:<br><br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | BASIC | CMDB | cmdb_rel_c | CIS v8 (9.7) CSF (DE.CM-4) ISO (8.7) NIST (SA-80) PCI (5.2.1, 5.4.1) CCM (TVM-02) |
| CIS Control V8 10.1 | Deploy and Maintain Anti-Malware Software:<br><br>Deploy and maintain anti-malware software on all enterprise assets. | BASIC | CMDB | cmdb_ci | CIS v8 (10.1) CSF (DE.CM-4) ISO (8.1, 8.7) NIST (SA-10) PCI (5.1.1, 5.2.1, 5.2.2, 5.3.2) CCM (TVM-02, UEM-09) |
| CIS Control V8 10.2 | Configure Automatic Anti-Malware Signature Updates:<br><br>Configure automatic updates for anti-malware signature files on all enterprise assets. | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| CIS Control V8 10.3 | Disable Autorun and Autoplay for Removable Media:<br><br>Disable autorun and autoplay auto-execute functionality for removable media. | BASIC | VR | sn_vulc_resul | CIS v8 (10.3) CSF (PR.PT-2) ISO (7.1) NIST (AC-18(1)) |
| CIS Control V8 10.4 | Configure Automatic Anti-Malware Scanning of Removable Media:<br><br>Configure anti-malware software to automatically scan removable media. | BASIC | VR | sn_vulc_resul | CIS v8 (10.4) CSF (DE.CM-4) ISO (7.1, 8.7) NIST (AC-18(3)) PCI (5.3.3) |
| CIS Control V8 10.5 | Enable Anti-Exploitation Features:<br><br>Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft Data Execution Prevention (DEP), Windows Defender Exploit Guard (WDEG), or Apple System Integrity Protection (SIP) and Gatekeeper™. | BASIC | VR | sn_vulc_resul | CIS v8 (10.5) CSF (DE.CM-4) ISO (8.7) NIST (CM-2) |
| CIS Control V8 10.6 | Centrally Manage Anti-Malware Software:<br><br>Centrally manage anti-malware software. | Manual | NA | NA | |
| CIS Control V8 10.7 | Use Behavior-Based Anti-Malware Software:<br><br>Use behavior-based anti-malware software. | BASIC | CMDB | cmdb_rel_ci | CIS v8 (10.7) CSF (DE.CM-4) ISO (8.1, 8.7) NIST (CM-7) PCI (5.3.2) |
| CIS Control V8 11.1 | Establish and Maintain a Data Recovery Process :<br><br>Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | | | | |
| CIS Control V8 11.2 | Perform Automated Backups :<br><br>Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data. | Manual | NA | NA | |
| CIS Control V8 11.3 | Protect Recovery Data:<br><br>Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements. | Manual | NA | NA | |
| CIS Control V8 11.4 | Establish and Maintain an Isolated Instance of Recovery Data :<br><br>Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services. | Manual | NA | NA | |
| CIS Control V8 11.5 | Test Data Recovery:<br><br>Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets. | Manual | NA | NA | |
| CIS Control V8 12.1 | Ensure Network Infrastructure is Up-to-Date:<br><br>Ensure network infrastructure is kept up-to-date. Example implementations include running | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support. | | | | |
| CIS Control V8 12.2 | Establish and Maintain a Secure Network Architecture:<br><br>Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. | Manual | NA | NA | |
| CIS Control V8 12.3 | Securely Manage Network Infrastructure:<br><br>Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS. | Manual | NA | NA | |
| CIS Control V8 12.4 | Establish and Maintain Architecture Diagram(s):<br><br>Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Manual | NA | NA | |
| CIS Control V8 12.5 | Centralize Network Authentication, Authorization, and Auditing (AAA):<br><br>Centralize network AAA. | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| CIS Control V8 12.6 | Use of Secure Network Management and Communication Protocols :<br><br>Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater). | BASIC | VR | sn_vulc_result | CIS v8 (12.6) CSF (PR.AC-7, PR.DS-2) ISO (8.21) NIST (SC-7(5)) |
| CIS Control V8 12.7 | Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure:<br><br>Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices. | Manual | NA | NA | |
| CIS Control V8 12.8 | Establish and Maintain Dedicated Computing Resources for All Administrative Work:<br><br>Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access. | Manual | NA | NA | |
| CIS Control V8 13.1 | Centralize Security Event Alerting:<br><br>Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard. | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| CIS Control V8 13.1 | Perform Application Layer Filtering:<br><br>Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway. | Manual | NA | NA | |
| CIS Control V8 13.11 | Tune Security Event Alerting Thresholds:<br><br>Tune security event alerting thresholds monthly, or more frequently. | Manual | NA | NA | |
| CIS Control V8 13.2 | Deploy a Host-Based Intrusion Detection Solution:<br><br>Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/ or supported. | BASIC | CMDB | cmdb_rel_c | CIS v8 (13.2) CSF (DE.CM-1) ISO (8.16) NIST (CM-6) PCI (6.4.2) |
| CIS Control V8 13.3 | Deploy a Network Intrusion Detection Solution:<br><br>Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service. | BASIC | CMDB | cmdb_ci | CIS v8 (13.3) CSF (DE.CM-1) ISO (8.16, 8.21) NIST (CM-7) PCI (11.5.1, 12.10.5) CCM (IVS-09) |
| CIS Control V8 13.4 | Perform Traffic Filtering Between Network Segments:<br><br>Perform traffic filtering between network segments, where appropriate. | Manual | NA | NA | |
| CIS Control V8 13.5 | Manage Access Control for Remote Assets: | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed; configuration compliance with the enterprise's secure configuration process; and ensuring the operating system and applications are up-to-date. | | | | |
| CIS Control V8 13.6 | Collect Network Traffic Flow Logs:<br><br>Collect network traffic flow logs and/or network traffic to review and alert upon from network devices. | Manual | NA | NA | |
| CIS Control V8 13.7 | Deploy a Host-Based Intrusion Prevention Solution:<br><br>Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent. | BASIC | CMDB | cmdb_ci | CIS v8 (13.7) CSF (DE.CM-1) ISO (8.8) NIST (AC-7) |
| CIS Control V8 13.8 | Deploy a Network Intrusion Prevention Solution:<br><br>Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service. | BASIC | CMDB | cmdb_ci | CIS v8 (13.8) CSF (DE.CM-1) ISO (8.8) NIST (AC-19) PCI (6.4.2, 11.5.1, 12.10.5) CCM (IVS-09) |
| CIS Control V8 13.9 | Deploy Port-Level Access Control:<br><br>Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network | BASIC | CMDB | cmdb_ci_endpoint_acl | CIS v8 (13.9) CSF (PR.AC-1) ISO (8.8) NIST (AC-19) PCI (1.2.1, |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | access control protocols, such as certificates, and may incorporate user and/or device authentication. | | | | 1.2.5, 1.2.6, 2.2.4) CCM (IVS-03) |
| CIS Control V8 14.1 | Establish and Maintain a Security Awareness Program:<br><br>Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard. | BASIC | Learning Core | sn_lc_user_course_activity | CIS v8 (14.1) CSF (ID.AM-6, ID.GV-1, PR.AT-1) ISO (6.3) NIST (SC-39) PCI (12.6, 12.6.1, 12.6.2, 12.6.3, 12.6.3.2) CCM (GRC-05, HRS-11, GRC-03) |
| CIS Control V8 14.2 | Train Workforce Members to Recognize Social Engineering Attacks:<br><br>Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating. | BASIC | Learning Core | sn_lc_user_course_activity | CIS v8 (14.2) CSF (PR.AT-1) ISO (8.7) PCI (12.6.3.1) CCM (HRS-11) |
| CIS Control V8 14.3 | Train Workforce Members on Authentication Best Practices:<br><br>Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management. | BASIC | Learning Core | sn_lc_user_course_activity | CIS v8 (14.3) CSF (PR.AT-1) ISO (6.3) PCI (8.3.8) CCM (GRC-05, HRS-11) |
| CIS Control V8 14.4 | Train Workforce on Data Handling Best Practices:<br><br>Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce | BASIC | Learning Core | sn_lc_user_course_activity | CIS v8 (14.4) CSF (PR.AT-1) ISO (5.1) NIST (AC-2) CCM (DSP-17, |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely. | | | | GRC-01, HRS-03, HRS-12) |
| CIS Control V8 14.5 | Train Workforce Members on Causes of Unintentional Data Exposure:<br><br>Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences. | BASIC | Learning Core | sn_lc_user_course_activity | CIS v8 (14.5) CSF (PR.AT-1) ISO (6.3) NIST (IA-5(1)) CCM (GRC-01, HRS-11) |
| CIS Control V8 14.6 | Train Workforce Members on Recognizing and Reporting Security Incidents:<br><br>Train workforce members to be able to recognize a potential incident and be able to report such an incident. | BASIC | Learning Core | sn_lc_user_course_activity | CIS v8 (14.6) CSF (PR.AT-1) ISO (6.8) NIST (AC-2(3)) CCM (HRS-11) |
| CIS Control V8 14.7 | Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates:<br><br>Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools. | BASIC | Learning Core | sn_lc_user_course_activity | CIS v8 (14.7) CSF (PR.AT-1) ISO (6.3) NIST (AC-6(2)) CCM (HRS-11) |
| CIS Control V8 14.8 | Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks: | BASIC | Learning Core | sn_lc_user_course_activity | CIS v8 (14.8) CSF (PR.AT-1) ISO (6.3) NIST |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure. | | | | (AC-6(5)) PCI (12.6.3.2) CCM (GRC-01, HRS-04) |
| CIS Control V8 14.9 | Conduct Role-Specific Security Awareness and Skills Training:<br><br>Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, (OWASP ™ Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles. | BASIC | Learning Core | sn_lc_user_course_activity | CIS v8 (14.9) CSF (PR.AT-1, PR.AT-2, R.AT-4, PR.AT-5) ISO (6.3) NIST (AC-2) PCI (9.5.1, 9.5.1.3, 12.10.40 CCM (HRS-09, HRS-12) |
| CIS Control V8 15.1 | Establish and Maintain an Inventory of Service Providers:<br><br>Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard. | BASIC | VRM | core_company | CIS v8 (15.1) CSF (ID.SC-2) ISO (5.19) NIST (AC-2(1)) PCI (12.8.1) CCM (STA-07) |
| CIS Control V8 15.2 | Establish and Maintain a Service Provider Management Policy:<br><br>Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard. | | | | |
| CIS Control V8 15.3 | Classify Service Providers:<br><br>Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard. | BASIC | VRM | core_company | CIS v8 (15.3) CSF (ID.SC-2) ISO (5.19) PCI (12.8.5) CCM (GRC-02, STA-08) |
| CIS Control V8 15.4 | Ensure Service Provider Contracts Include Security Requirements:<br><br>Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements. | Manual | NA | NA | |
| CIS Control V8 15.5 | Assess Service Providers:<br><br>Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), | BASIC | VRM | core_company | CIS v8 (15.5) CSF (ID.SC-4, ID.SC-2) ISO (5.19) NIST (IA-5) PCI (12.8.3) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Indicator templates for CIS v8 Controls (continued)**

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts. | | | | CCM (STA-12, STA-13) |
| CIS Control V8 15.5 | Assess Service Providers:<br><br>Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts. | BASIC | VRM | core_company | CIS v8 (15.5) CSF (ID.SC-4, ID.SC-2) ISO (5.22, 5.23) NIST (IA-5) PCI (12.8.30) CCM (STA-12, STA-13) |
| CIS Control V8 15.6 | Monitor Service Providers:<br><br>Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring. | BASIC | VRM | core_company | CIS v8 (15.6) CSF (DE.CM-6) ISO (5.2, 5.19, 5.21, 5.22) NIST (AC-1) PCI (8.2.7, 12.4.2, 12.4.2.1, 12.8.4 CCM (STA-14) |
| CIS Control V8 15.7 | Securely Decommission Service Providers:<br><br>Securely decommission service providers. Example | BASIC | VRM | core_company | CIS v8 (15.7) CSF (PR.AC-1) ISO (5.19, 5.2) NIST |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems. | | | | (AC-2, AC-2(1)) |
| CIS Control V8 16.1 | Establish and Maintain a Secure Application Development Process:<br><br>Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Manual | NA | NA | |
| CIS Control V8 16.1 | Apply Secure Design Principles in Application Architectures:<br><br>Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | and files, and renaming or removing default accounts. | | | | |
| CIS Control V8 16.11 | Leverage Vetted Modules or Services for Application Security Components:<br><br>Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs. | Manual | NA | NA | |
| CIS Control V8 16.12 | Implement Code-Level Security Checks:<br><br>Apply static and dynamic analysis tools within the application lifecycle to verify that secure coding practices are being followed. | Manual | NA | | |
| CIS Control V8 16.13 | Conduct Application Penetration Testing:<br><br>Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user. | | | | |
| CIS Control V8 16.14 | Conduct Threat Modeling:<br><br>Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses. | Manual | NA | NA | |
| CIS Control V8 16.2 | Establish and Maintain a Process to Accept and Address Software Vulnerabilities:<br><br>Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant | BASIC | VR | sn_vul_remediation_task | CIS v8 (16.2) CSF (RS.AN-5) ISO (8.8) NIST (AC-2) PCI (6.3.1) CCM (AIS-07, AIS-03) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | enterprise changes occur that could impact this Safeguard. | | | | |
| CIS Control V8 16.3 | Perform Root Cause Analysis on Security Vulnerabilities:<br><br>Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise. | Manual | NA | NA | |
| CIS Control V8 16.4 | Establish and Manage an Inventory of Third-Party Software Components:<br><br>Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate the component is still supported. | Manual | NA | NA | |
| CIS Control V8 16.5 | Use Up-to-Date and Trusted Third-Party Software Components:<br><br>Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | or evaluate the software for vulnerabilities before use. | | | | |
| CIS Control V8 16.6 | Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities:<br><br>Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually. | BASIC | VR | sn_vul_vulnerable_item | CIS v8 (16.6) CSF (RS.AN-1) ISO (8.8) NIST (AC-19) PCI (6.3.1) CCM (AIS-07, TVM-08) |
| CIS Control V8 16.7 | Use Standard Hardening Configuration Templates for Application Infrastructure:<br><br>Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening. | Manual | NA | NA | |
| CIS Control V8 16.8 | Separate Production and Non-Production Systems:<br><br>Maintain separate environments for production and non-production systems. | SCRIPTED | CMDB | cmdb_ci | CIS v8 (16.8) CSF (PR.DS-7) ISO (8.31) NIST (IA-2(2)) PCI (6.5.3) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | | | | | CCM (IVS-05) |
| CIS Control V8 16.9 | Train Developers in Application Security Concepts and Secure Coding:<br><br>Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers. | BASIC | Learning Core | sn_lc_user_course_activity | CIS v8 (16.9) CSF (PR.AT-1, PR.AT-2) ISO (8.28) NIST (IA-2(1)) PCI (6.2.2) |
| CIS Control V8 17.1 | Designate Personnel to Manage Incident Handling:<br><br>Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | BASIC | SIR | sys_user_has_role | CIS v8 (17.1) CSF (PR.IP-9, DE.DP-1) ISO (5.24) NIST (AC-5) PCI (12.10.3, 12.10.4) CCM (BCR-01, SEF-03) |
| CIS Control V8 17.2 | Establish and Maintain Contact Information for Reporting Security Incidents: | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date. | | | | |
| CIS Control V8 17.3 | Establish and Maintain an Enterprise Process for Reporting Incidents:<br><br>Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | BASIC | SIR | kb_knowledge | CIS v8 (17.3) CSF (PR.IP-9, PR.AT-1) ISO (6.8) NIST (AC-6(1)) PCI (12.10) |
| CIS Control V8 17.4 | Establish and Maintain an Incident Response Process:<br><br>Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | Manual | SIR | NA | |
| CIS Control V8 17.5 | Assign Key Roles and Responsibilities: | BASIC | SIR | sys_user_has_role | CIS v8 (17.5) CSF (DE.DP-4, RS.CO-2, |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | | | | RS.CO-3, RS.CO-4) ISO (5.2, 5.24) NIST (AU-9(4)) PCI (12.10.3) CCM (SEF-03) |
| CIS Control V8 17.6 | Define Mechanisms for Communicating During Incident Response:<br><br>Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | Manual | NA | NA | |
| CIS Control V8 17.7 | Conduct Routine Incident Response Exercises:<br><br>Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision making, and workflows. Conduct testing on an annual basis, at a minimum. | Manual | NA | NA | |
| CIS Control V8 17.8 | Conduct Post-Incident Reviews:<br><br>Conduct post-incident reviews. Post-incident reviews help | Manual | NA | NA | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates for CIS v8 Controls (continued)

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | prevent incident recurrence through identifying lessons learned and follow-up action. | | | | |
| CIS Control V8 17.9 | Establish and Maintain Security Incident Thresholds:<br><br>Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | BASIC | SIR | sn_si_calculator | CIS v8 (17.9) CSF (RS.AN-5) ISO (5.24, 5.25) NIST (RA-5) PCI (12.10.5) CCM (SEF-05) |
| CIS Control V8 18.1 | Establish and Maintain a Penetration Testing Program:<br><br>Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements. | Manual | NA | NA | |
| CIS Control V8 18.2 | Perform Periodic External Penetration Tests:<br><br>Perform periodic external penetration tests based on program requirements, no less than annually. External | BASIC | VR | sn_vul_remediation_task | CIS v8 (18.2) ISO (8.8) NIST (RA-7) PCI (11.4.3) |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Indicator templates for CIS v8 Controls (continued)**

| Control | Name/Description | Type | Compliance validated by | Source table | Related control objectives |
|---|---|---|---|---|---|
| | penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box. | | | | |
| CIS Control V8 18.3 | Remediate Penetration Test Findings:<br><br>Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization. | Manual | NA | NA | |
| CIS Control V8 18.4 | Validate Security Measures:<br><br>Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing. | Manual | NA | NA | |
| CIS Control V8 18.5 | Perform Periodic Internal Penetration Tests:<br><br>NA | BASIC | VR | sn_vul_remediation_task | CIS v8 (18.5) ISO (8.8) NIST (RA-5) PCI (11.4.2) |

## Indicator templates for CIS v7 Controls

The following tables list the Basic and Script indicator templates for CIS v7 Controls.

**Note:** Controls currently not covered by either basic or scripted indicator templates have manual indicator templates defined for the purposes of compliance validation.

**Basic indicator templates for CIS v7 Controls**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| CIS Control 1.1 | Utilize an Active Discovery Tool: | Configuration Management (CMDB) | CMDB Discovery [cmdb_discovery] | 07054 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Basic indicator templates for CIS v7 Controls (continued)

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory. | | | 00693 |
| CIS Control 1.2 | Use a Passive Asset Discovery Tool:<br><br>Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory. | Discovery | Network Discovery Tracking [discovery_network_track] | 01472 |
| CIS Control 1.4 | Maintain Detailed Asset Inventory:<br><br>Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not. | Configuration Management (CMDB) | Hardware [cmdb_ci_hardware] | 06631<br><br>00691 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| CIS Control 1.5 | Maintain Asset Inventory Information:<br><br>Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network. | Configuration Management (CMDB) | Base Configuration Item [cmdb] | 06638<br><br>06640<br><br>12084<br><br>06636<br><br>13721<br><br>13722 |
| CIS Control 1.7 | Deploy Port Level Access Control:<br><br>Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network. | Configuration Management (CMDB) | ACL Endpoint [cmdb_ci_endpoint_acl] | 11841<br><br>13718 |
| CIS Control 1.8 | Utilize Client Certificates to Authenticate Hardware Assets: | Certification Core | Audit [cert_audit] | 01429 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | Use client certificates to authenticate hardware assets connecting to the organization's trusted network. | | | |
| CIS Control 2.1 | Maintain Inventory of Authorized Software:<br><br>Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system. | Configuration Management (CMDB) | Application Software [cmdb_ci_application_software] | 12093<br>13723 |
| CIS Control 2.2 | Ensure Software is Supported by Vendor:<br><br>Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system. | Software Asset Management | Software Product Lifecycle [sam_sw_product_lifecycle] | 07054 |
| CIS Control 2.3 | Utilize Software Inventory Tools: | Configuration Management (CMDB) | Application Software [cmdb_ci_application_software] | 11736<br>12196 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Basic indicator templates for CIS v7 Controls (continued)

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems. | | | 13720<br>13725 |
| CIS Control 2.4 | Track Software Inventory Information:<br>The software inventory system should track the name, version, publisher, and installation date for all software, including operating systems authorized by the organization. | Software Asset Management Core | Software Installation [cmdb_sam_sw_install] | 12085 |
| CIS Control 2.5 | Integrate Software and Hardware Asset Inventories:<br>The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location. | Configuration Management (CMDB) | Application Software [cmdb_ci_application_software] | 11637<br>11857 |
| CIS Control 3.1 | Run Automated Vulnerability Scanning Tools:<br>Utilize an up-to-date SCAP-compliant vulnerability | Vulnerability Response | Vulnerability Data Source Import Queue Entry [sn_vul_ds_import_q_entry] | 10635 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems. | | | |
| CIS Control 3.2 | Perform Authenticated Vulnerability Scanning:<br><br>Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested. | Security Operations | Discovered Item [sn_sec_cmn_src_ci] | 00706 |
| CIS Control 3.6 | Compare Back-to-back Vulnerability Scans:<br><br>Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner. | Vulnerability Response | Vulnerability Remediation Status [sn_vul_m2m_ttr_status] | 06080 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| CIS Control 4.2 | Change Default Passwords<br><br>Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts. | Configuration Compliance | Configuration Test [sn_vulc_test] | 01698<br><br>12122 |
| CIS Control 4.4 | Use Unique Passwords<br><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system. | Configuration Compliance | Configuration Test [sn_vulc_test] | 01915<br><br>01337 |
| CIS Control 4.8 | Log and Alert on Changes to Administrative Group Membership<br><br>Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges. | Configuration Compliance | Configuration Test [sn_vulc_test] | 06312 |
| CIS Control 4.9 | Log and Alert on Unsuccessful Administrative Account Login | Configuration Compliance | Configuration Test [sn_vulc_test] | 06312<br><br>06331 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account. | | | |
| CIS Control 6.2 | Activate audit logging:<br><br>Ensure that local logging has been enabled on all systems and networking devices. | Configuration Compliance | Configuration Test [sn_vulc_test] | 00897 |
| CIS Control 6.3 | Enable Detailed Logging:<br><br>Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. | Configuration Compliance | Configuration Test [sn_vulc_test] | 00575 |
| CIS Control 7.1 | Ensure Use of Only Fully Supported Browsers and Email Clients:<br><br>Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers | Vulnerability Response | Application Vulnerable Item [sn_vul_app_vulnerable_item] | 00575<br>00576 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | and email clients provided by the vendor. | | | |
| CIS Control 8.1 | Utilize Centrally Managed Anti-malware Software<br><br>Any enterprise class AV software will have this capability. By having a centrally managed AV, you can easily enable individual requirements. | Configuration Compliance | Configuration Test [sn_vulc_test] | 11861 |
| CIS Control 8.2 | Ensure Anti-Malware Software and Signatures are Updated<br><br>The AV is only as good as it's signatures. While pure signature-based detection is no longer viable, even anomaly-based engines need to be updated on a regular basis. Ensure that the updates are rolled out automatically and use tools to verify that the signatures are actually up-to-date. | Configuration Compliance | Configuration Test [sn_vulc_test] | 01790 |
| CIS Control 8.3 | Enable Operating System Anti- | Configuration Compliance | Configuration Test [sn_vulc_test] | 11637 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | Exploitation Features/ Deploy Anti-Exploit Technologies<br><br>The DISA hardening guides provide step-by-step instructions on enabling these settings and so much more. | | | 10678 |
| CIS Control 8.4 | Configure Anti-Malware Scanning of Removable Devices<br><br>Most AVs have this capability turned on by default, but it's still important to verify that it's actually still enabled. Malware coming in via a USB stick is a viable attack vector for nearly every organization. | Configuration Compliance | Configuration Test [sn_vulc_test] | 11927<br><br>04824<br><br>06735<br><br>00561<br><br>00564<br><br>04546 |
| CIS Control 8.5 | Configure Devices Not To Auto-run Content<br><br>For the same reason why you do not want to scan it, you also don't want it to run when it's mounted. This is a pretty quick setting to enable, and both CIS and DISA hardening | Configuration Compliance | Configuration Test [sn_vulc_test] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | guides have step-by-step instructions on disabling auto-run. Some SCM tools can quickly check every endpoint in your environment to make sure this setting is disabled. | | | |
| CIS Control 9.3 | Perform Regular Automated Port Scans:<br><br>Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system. | Vulnerability Response | Vulnerability Scanner [sn_vul_scanner] | N/A |
| CIS Control 11.3 | Use Automated Tools to Verify Standard Device Configurations and Detect Changes<br><br>Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered. | Configuration Compliance | Configuration Test [sn_vulc_test] | 06428<br><br>07058 |
| CIS Control 11.4 | Install the Latest Stable Version | Vulnerability Response | Vulnerable Item [sn_vul_vulnerable_item] | 01696 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | of Any Security-related Updates on All Network Devices:<br><br>Install the latest stable version of any security-related updates on all network devices. | | | |
| CIS Control 12.6 | Deploy Network-based IDS Sensor:<br><br>Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries. | Configuration Management (CMDB) | Intrusion Detection System [cmdb_ci_ids_network] | 00581 |
| CIS Control 13.2 | Remove Sensitive Data or Systems Not Regularly Accessed by Organization:<br><br>Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the | Configuration Compliance | Configuration Test [sn_vulc_test] | 13726<br><br>13727 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed. | | | |
| CIS Control 13.9 | Encrypt Data on USB Storage Devices<br><br>Provide the training to employees so they are aware of the risks of data on USB drives. Then provide them with the tools to secure your organization's critical data. | Configuration Compliance | Configuration Test [sn_vulc_test] | 11927 |
| CIS Control 14.4 | Encrypt All Sensitive Information in Transit:<br><br>Encrypt all sensitive information in transit. | Configuration Compliance | Configuration Test [sn_vulc_test] | 00564 |
| CIS Control 15.1 | Maintain an Inventory of Authorized Wireless Access Points:<br><br>Maintain an inventory of authorized wireless access points connected to the wired network. | Configuration Management (CMDB) | Wireless Access Point [cmdb_ci_wap_network] | 00693 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| CIS Control 16.1 | Maintain an Inventory of Authentication Systems:<br><br>Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider. | Configuration Management (CMDB) | Active Directory Domain Controller [cmdb_ci_ad_controller] | 13724 |
| CIS Control 16.4 | Encrypt or Hash all Authentication Credentials:<br><br>Encrypt or hash with a salt all authentication credentials when stored. | Configuration Compliance | Configuration Test [sn_vulc_test] | 06735 |
| CIS Control 16.5 | Encrypt Transmittal of Username and Authentication Credentials:<br><br>Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. | Configuration Compliance | Configuration Test [sn_vulc_test] | 00564 |
| CIS Control 16.11 | Lock Workstation Sessions After Inactivity:<br><br>Automatically lock workstation sessions after a standard period of inactivity. | Configuration Compliance | Configuration Test [sn_vulc_test] | 04490 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| CIS Control 16.13 | Alert on Account Login Behavior Deviation:<br><br>Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration. | Security Incident Response | Security Incident [sn_si_incident] | 07068<br><br>07070<br><br>07069 |
| CIS Control 18.5 | Use Only Standardized and Extensively Reviewed Encryption Algorithms:<br><br>Use only standardized and extensively reviewed encryption algorithms. | CMDB CI Class Models | Unique Certificate [cmdb_ci_certificate] | 00037 |
| CIS Control 18.8 | Establish a Process to Accept and Address Reports of Software Vulnerabilities:<br><br>Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group. | Vulnerability Response | Discovery Model Vulnerable Software Match [sn_vul_discovery_model_software_match] | 04810 |
| CIS Control 19.2 | Assign Job Titles and Duties for Incident Response: | Incident Management | User Roles [sys_user_has_role] | 07061<br><br>00691 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for CIS v7 Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution. | | | |
| CIS Control 19.3 | Designate Management Personnel to Support Incident Handling:<br><br>Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles. | Incident Management | User Roles [sys_user_has_role] | 01211 |
| CIS Control 19.6 | Publish Information Regarding Reporting Computer Anomalies and Incidents:<br><br>Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. | Security Incident Response | Knowledge [kb_knowledge] | 12093 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Basic indicator templates for CIS v7 Controls (continued)

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | Such information should be included in routine employee awareness activities. | | | |
| CIS Control 19.8 | Create Incident Scoring and Prioritization Schema:<br><br>Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments. | Security Incident Response | Security Incident Calculator [sn_si_calculator] | 12093<br><br>13723 |

### Script indicator templates for CIS v7 Controls

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| CIS Control 18.9 | Separate Production and Non-Production Systems:<br><br>Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments. | Configuration Management (CMDB) | Configuration Item [cmdb_ci] | 00922 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Indicator templates for ISO Controls

The following tables list the Basic and Script indicator templates for ISO Controls.

**Note:** Controls currently not covered by either basic or scripted indicator templates have manual indicator templates defined for the purposes of compliance validation.

### Basic indicator templates for ISO Controls

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| ISO27002 - 5.1.1 | Policies for information security:<br><br>Define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives. The information security policy are supported by topic-specific policies, which further mandate the implementation of information security controls to include: access control; information classification (and handling); physical and environmental security; backup; information transfer; protection from malware; management of technical vulnerabilities; cryptographic controls; | GRC: Policy and Compliance Management | Compliance Policy [sn_compliance_policy] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | communications security; privacy and protection of personally identifiable information; supplier relationships and end user oriented topics such as: 1) acceptable use of assets; 2) clear desk and clear screen; 3) information transfer; 4) mobile devices and teleworking; 5) restrictions on software installations and use. | | | |
| ISO27002 - 6.1.1 | Information security roles and responsibilities:<br><br>Ensure responsibilities for the protection of individual assets are identified in the asset inventory. Ensure roles and responsibilities for the development and implementation of information security are clearly defined. | GRC: Policy and Compliance Management | Control [sn_compliance_control] | N/A |
| ISO27002 - 6.2.1 | Mobile device policy:<br><br>Utilize approved whole disk encryption | GRC: Policy and Compliance Management | Compliance Policy [sn_compliance_policy] | 07054<br>01472<br><br>12109 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | software to encrypt the hard drive of all mobile devices. | | | 06631<br>00691<br>06638<br>06640<br>12084<br>06636<br>13721<br>13722<br>12093<br>11736<br>12196<br>13720<br>13725<br>00693<br>13724 |
| ISO27002 - 6.2.2 | Teleworking:<br><br>Enforce remote access policies for employees and contractors. | GRC: Policy and Compliance Management | Compliance Policy [sn_compliance_policy] | N/A |
| ISO27002 - 7.1.1 | Screening:<br><br>Ensure background verification check are performed for all employees and contractors prior to granting access to company's assets. | Human Resources: Core | HR Talent Management Cases [sn_hr_core_case_talent_management] | 12001<br>00897<br>04490<br>12100<br>12099<br>04594<br>04476 |
| ISO27002 - 7.1.2 | Terms and conditions of employment: | Human Resources: Core | sn_hr_core_task | 01429 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | Ensure all new hire employees or contractors signed and agreed to the terms and conditions of employment, including their responsibility for information security. | | | |
| ISO27002 - 8.1.1 | Inventory of assets:<br><br>Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network. | Configuration Management (CMDB) | Base Configuration Item [cmdb] | 00562<br><br>00561<br><br>01915<br><br>01337<br><br>01421<br><br>06440 |
| ISO27002 - 8.1.2 | Ownership of assets:<br><br>Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether | Configuration Management (CMDB) | Base Configuration Item [cmdb] | 06080<br><br>01273 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | the hardware asset has been approved to connect to the network. | | | |
| ISO27002 - 8.1.3 | Acceptable use of assets:<br><br>Ensure employees and contractors are made aware of the information security requirements of the organizations assets associated with information and information processing facilities and resources. They should be responsible for their use of any information processing resources and of any such use carried out under their responsibility. | GRC: Policy and Compliance Management | Compliance Policy [sn_compliance_policy] | 12001<br>00897<br>04490<br>12100<br>12099<br>04594<br>04476 |
| ISO27002 - 9.3.1 | Use of secret authentication information:<br><br>Use client certificates to authenticate hardware assets connecting to the organization's trusted network. | Configuration Compliance | Configuration Test [sn_vulc_test] | 01429 |
| ISO27002 - 9.4.2 | Secure log-on procedures: | Configuration Compliance | Configuration Test [sn_vulc_test] | 00562<br>00561 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication. | | | 01915<br>01337<br>01421<br>06440 |
| ISO27002 - 9.4.3 | Password management system:<br><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system. | Configuration Compliance | Configuration Test [sn_vulc_test] | 06080<br>01273 |
| ISO27002 - 10.1.1 | Policy on the use of cryptographic controls:<br><br>Ensure policy surrounding encryption exist and are applied, implemented and enforced in accordance to data classification requirements. | GRC: Policy and Compliance Management | Compliance Policy [sn_compliance_policy] | 07058<br>06428 |
| ISO27002 - 10.1.2 | Key management:<br><br>Ensure management of encryption keys are managed following a formal policy and procedure | GRC: Policy and Compliance Management | Compliance Policy [sn_compliance_policy] | 00897<br>00575<br>00576<br>11861<br>01790 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | for the entire lifecycle of the key. | | | |
| ISO27002 - 11.2.9 | Clear desk and clear screen policy:<br><br>Ensure clear desk policy is adapted by employees and contractors. | GRC: Policy and Compliance Management | Compliance Policy [sn_compliance_policy] | 06312<br>00577<br><br>12210 |
| ISO27002 - 12.1.2 | Controls against malware:<br><br>Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor. | Configuration Compliance | Configuration Test [sn_vulc_test] | N/A |
| ISO27002 - 12.2.1 | Controls against malware:<br><br>Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor. | Configuration Compliance | Configuration Test [sn_vulc_test] | N/A |
| ISO27002 - 12.4.1 | Event logging:<br><br>Ensure that local logging has been enabled | Instance Security Center | Security Dashboard Event Logs [appsec_security_dashboard_event_logs] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | on all systems and networking devices. | | | |
| ISO27002 - 12.4.2 | Protection of log information:<br><br>Ensure logs are securely protected from unauthorized access. | | Access Roles [sys_security_acl_role] | N/A |
| ISO27002 - 12.4.3 | Administrator and operator logs:<br><br>Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring). | Configuration Compliance | Configuration Test [sn_vulc_test] | N/A |
| ISO27002 - 13.2.1 | Information transfer policies and procedures:<br><br>Ensure formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities. | GRC: Policy and Compliance Management | Compliance Policy [sn_compliance_policy] | N/A |
| ISO27002 - 14.1.1 | Information security requirements | GRC: Advanced Risk | Risk Assessments [sn_risk_advanced_risk_assessment_instance] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | analysis and specification:<br><br>Ensure information security related requirements are included in the requirements for new information systems or enhancements to existing information systems. | | | |
| ISO27002 - 14.2.2 | Technical review of applications after operating platform changes:<br><br>Ensure business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security when ever there are changes to the operating platforms. | Change Request | Change Request [change_request] | N/A |
| ISO27002 - 14.2.3 | Restrictions on changes to software packages:<br><br>Ensure modifications to software packages are discouraged, or limited to necessary changes and all changes | Change Request | Change Request [change_request] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | are strictly controlled. | | | |
| ISO27002 - 14.2.4 | System security testing:<br><br>Ensure security testing such as secure code reviews and vulnerability scan are performed during development lifecycle. Ensure identified vulnerabilities are documented and remediation are performed. | Change Request | Change Request [change_request] | N/A |
| ISO27002 - 14.2.8 | System acceptance testing:<br><br>Ensure system acceptance testing includes testing of information security requirements and adherence to secure system development practices. | DevOps | Build Test Results [sn_devops_build_test_result] | N/A |
| ISO27002 - 14.2.9 | System acceptance testing:<br><br>Ensure system acceptance testing includes testing of information security requirements and adherence to secure system | DevOps | Task Executions [sn_devops_task_execution] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | development practices. | | | |
| ISO27002 - 15.1.1 | Information security policy for supplier relationships:<br><br>Ensure information security controls are addressed and resolved with the supplier prior to conducting business or granting vendor access to assets. | GRC: Vendor Risk Management | Vendor Risk Assessment [sn_vdr_risk_asmt_assessment | N/A<br>sn_vdr_risk_asmt_asses |
| ISO27002 - 15.1.3 | Information and communication technology supply chain:<br><br>Ensure risk assessment are performed to prior to doing business and granting suppliers and vendors access to assets and security controls and requirements are agreed upon and documented in the suppliers/ vendors agreement. | GRC: Vendor Risk Management | Vendor Risk Assessment [sn_vdr_risk_asmt_assessment | N/A<br>sn_vdr_risk_asmt_asses |
| ISO27002 - 15.2.1 | Monitoring and review of supplier services:<br><br>Ensure supplier are regularly monitoring and review to | GRC: Vendor Risk Management | Vendor Risk Assessment [sn_vdr_risk_asmt_assessment | N/A<br>sn_vdr_risk_asmt_asses |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Basic indicator templates for ISO Controls (continued)

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly. | | | |
| ISO27002 - 15.2.2 | Managing changes to supplier services:<br><br>Ensure 3rd Party risk assessment are performed when ever there are changes to provision of services. Ensure changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, are managed. | GRC: Vendor Risk Management | Repeating Assessments [sn_vdr_risk_asmt_repeating_assessment] | N/A |
| ISO27002 - 16.1.2 | Reporting information security events:<br><br>Ensure there is a formal Incident Management program in place and all personnel and third parties are trained on how to | Security Incident Response | Security Incident [sn_si_incident] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Basic indicator templates for ISO Controls (continued)

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | recognize and report security incidents. | | | |
| ISO27002 - 16.1.4 | Assessment of and decision on information security events:<br><br>Ensure there is a formal information security event management to include agreed security event and incident classification scale for reporting and escalation. Ensure threat and risk classification scheme are documented. Ensure incident response notifications are maintained. Ensure impact thresholds to be used in categorizing incidents are documented. | Security Incident Response | Security Incident [sn_si_incident] | N/A |
| ISO27002 - 16.1.5 | Response to information security incidents:<br><br>Ensure information security incidents are responded to and managed in accordance with the documented procedures. | Security Incident Response | Security Incident [sn_si_incident] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Basic indicator templates for ISO Controls (continued)

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| ISO27002 - 16.1.6 | Learning from information security incidents:<br><br>Ensure incident monitoring procedures are included in the Incident Management Program to document incidents and ensuring security event are periodically analyzed to reduce future incident. | Security Incident Response | Security Incident [sn_si_incident] | N/A |
| ISO27002 - 17.1.1 | Planning information security continuity:<br><br>Ensure information security and the continuity of information security management are planned and included in business continuity plan or within the disaster recovery plan. | GRC: Business Impact Analysis | Impact Analysis [sn_bia_analysis] | N/A |
| ISO27002 - 17.1.2 | Implementing information security continuity:<br><br>Ensure business continuity or disaster recovery plan are formally documented. | GRC: Business Impact Analysis | Impact Analysis [sn_bia_analysis] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Basic indicator templates for ISO Controls (continued)

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| ISO27002 - 17.1.3 | Verify, review and evaluate information security continuity:<br><br>Ensure business continuity or disaster recovery plan are annual exercise to validate adequate security control are valid and effective during adverse situation. | GRC: Business Impact Analysis | Impact Analysis [sn_bia_analysis] | N/A |
| ISO27002 - 17.2.1 | Availability of information processing facilities:<br><br>Ensure failover and recovery components work as intended. | GRC: Crisis Management | Events [sn_recovery_event] | N/A |
| ISO27002 - 18.1.3 | Protection of records:<br><br>Ensure records and data are protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements. | GRC: Policy and Compliance Management | Compliance Policy [sn_compliance_policy] | N/A |
| ISO27002 - 18.1.4 | Privacy and protection of personally | GRC: Policy and Compliance Management | Compliance Policy [sn_compliance_policy] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Basic indicator templates for ISO Controls (continued)**

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | identifiable information:<br><br>Ensure privacy and protection of personally identifiable information are protected and handled in accordance with legislation and regulation where applicable. | | | |
| ISO27002 - 18.2.2 | Compliance with security policies and standards:<br><br>Ensure testing of in scope systems configuration against compliance and regulatory requirements are regularly performed. Ensure baseline configuration standards for systems are documented and based upon industry best practices. | Configuration Compliance | Policies [sn_vulc_policy] | 01422<br><br>01355 |
| ISO27002 - 18.2.3 | Technical compliance review:<br><br>Ensure periodic vulnerability scan and penetration test are performed and testing of in scope systems configuration against | Configuration Compliance | Test Results [sn_vulc_result] | N/A |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Basic indicator templates for ISO Controls (continued)

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| | compliance and regulatory requirements. | | | |

### Script indicator templates for ISO Controls

| Control | Name/Description | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|
| ISO27002 - 8.1.4 | Return of assets:<br><br>Ensure the termination process is formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization. | Human Resources: Core Asset Management | • HR Profiles [sn_hr_core_profile]<br>• Asset [alm_asset] | N/A |
| ISO27002 - 12.1.4 | Separation of development, testing and operational environments:<br><br>Maintain separate environments for production and nonproduction systems. Developers should not have unmonitored access to production environments. | Configuration Management (CMDB) | Configuration Item [cmdb_ci] | 01698<br><br>12122<br><br>00644<br><br>00596 |

## Indicator templates common to CIS and ISO Controls

The following tables list the Basic and Script indicator templates that are common to both CIS and ISO Controls.

**Note:** Controls currently not covered by either basic or scripted indicator templates have manual indicator templates defined for the purposes of compliance validation.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Indicator templates common to CIS and ISO Controls

| Control | Name/ Description | Indicator template type | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|---|
| CIS Control 2.6, ISO27002 - 12.5.1 | Address unapproved software:<br><br>Ensure software assets are managed and regularly updated. | Script | • Software Asset Management Core<br>• Software Asset Management Professional Core | • Software Installation [cmdb_sam_sw_install]<br>• Software Models [cmdb_software_product_model] | 11637<br><br>00656<br><br>11624 |
| CIS Control 3.7, ISO27002 - 12.6.1 | Utilize a Risk-rating Process:<br><br>Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities. | Basic | Vulnerability Response | Vulnerable Item [sn_vul_vulnerable_item] | 01273 |
| CIS Control 7.2, ISO27002 - 12.6.2 | Restrictions on software installation:<br><br>Uninstall or disable any unauthorized browser or email client plugins or add-on applications. | Script | • Software Asset Management Core<br>• Software Asset Management Professional Core | • Software Installation [cmdb_sam_sw_install]<br>• Software Models [cmdb_software_product_model] | 00575<br><br>00574 |
| CIS Controls 18.1, ISO27002 - 14.2.1 | Establish Secure Coding Practices:<br><br>Establish secure coding practices appropriate to the programming language and development | Basic | GRC: Policy and Compliance Management | Policy [sn_compliance_policy] | 11863 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Indicator templates common to CIS and ISO Controls (continued)**

| Control | Name/ Description | Indicator template type | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|---|
| | environment being used. | | | | |
| CIS Control 19.1, ISO27002 - 16.1.1 | Document Incident Response Procedures:<br><br>Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/ management. | Basic | Security Incident Response | Security Incident [sn_si_incident] | 11780 |
| CIS Control 19.4, ISO27002 - 16.1.3 | Reporting information security weaknesses:<br><br>Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the | Basic | Security Incident Response | Security Incident [sn_si_incident] | 07183<br><br>12975<br><br>10033 |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Indicator templates common to CIS and ISO Controls (continued)**

| Control | Name/ Description | Indicator template type | Compliance validated by | Source table | Related UCF IDs |
|---|---|---|---|---|---|
| | incident notification. | | | | |

## 360° Relationship Visualization

The 360° Relationship Visualization application allows you to visually explore the relationships between the different types of critical data that affect your business, such as controls, risks, and issues. The visualization also facilitates quick actions upon the information, such as adding a relationship, closing an issue, or approving a policy exception.

Before you can use the 360° Relationship Visualization application, you must set up the data registry to define the kinds of relationships to be viewed and to configure the views of the data to be shown in the 360° View.

### Who uses the 360° Relationship Visualization

360° Relationship Visualization is used by GRC practitioners, such as compliance managers and analysts, risk managers and analysts, and auditors. 360° Relationship Visualization helps GRC practitioners to understand the critical data that affects their business. It also aids in effectively communicating the relationships and their impacts to C-suite executives or business users such as application or business service owners.

This table contains the responsibilities of all stakeholders involved with the 360° Relationship Visualization application and the Data Registry.

**360° Relationship Visualization and Data Registry roles and responsibilities**

| Role title | Description | Contains roles |
|---|---|---|
| Data registry administrator [sn_data_registry.admin] | The data registry administrator has CRUD access to all records in the 360° views. | csn_data_registry.reader |
| Data registry reader [sn_data_registry.reader] | The data registry reader role must be granted to all GRC users (for example, ompliance managers and analysts, risk managers and analysts, and auditors) who are working on 360° Relationship Visualization-enabled GRC forms. | • canvas_user<br>• workspace_user |

### Download and activate the GRC: 360° Relationship Visualization and Data Registry applications

Before you can run the GRC: 360° Relationship Visualization (com.servicenow_sn_grc_360_degree_visualization) and Data Registry (com.sn_app_grc_data_registry) applications in your instance, you must download them from the ServiceNow Store.

**Before you begin**
Role required: admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Procedure

Follow the instructions for Download a GRC application from the ServiceNow Store for the first time.

## Setting up the 360° views

To effectively use the 360° Relationship Visualization application, you need to register existing relationships between the types of data you want to view, and then configure how the 360° view displays that data.

### Register 360° relationships

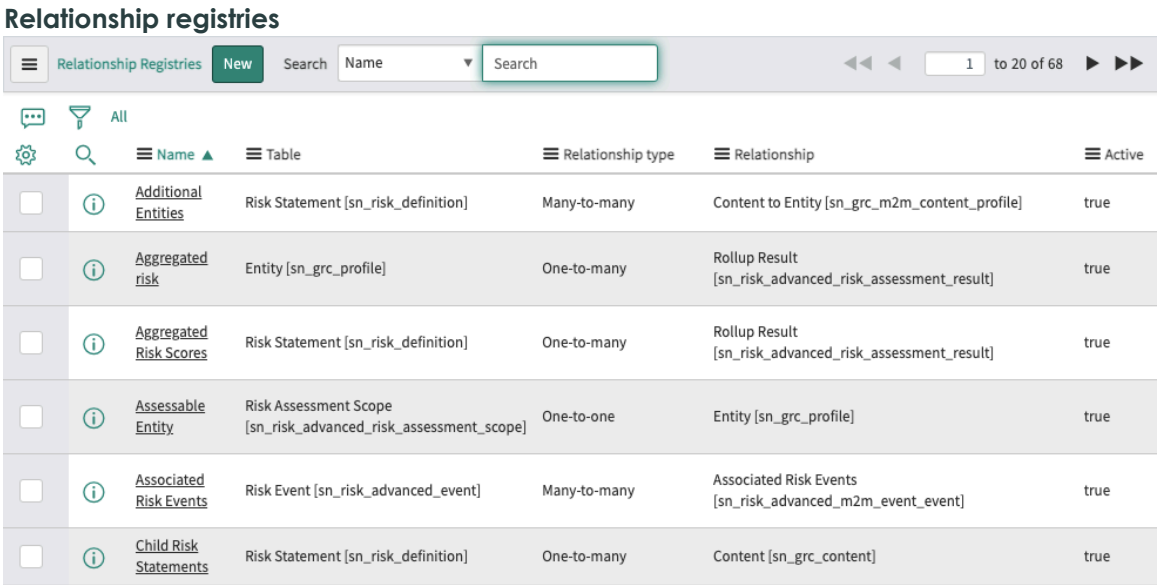
The first step in setting up your data registry is to register the relationships you want displayed in the 360° Relationship Visualization.

### Before you begin

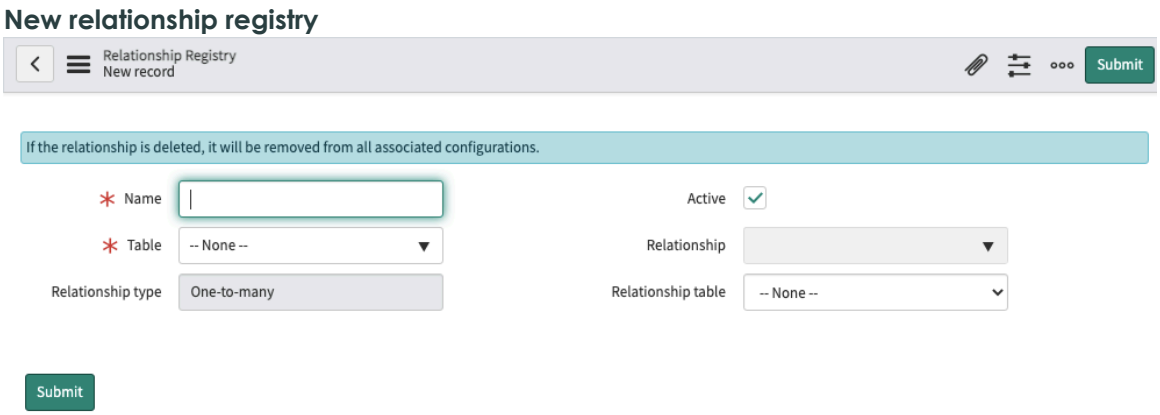
Role required: Data registry administrator

### Procedure

1. Navigate to **360° View Configurations** > **Relationship Registries**.




2. Click **New**.




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. On the form, fill in the fields.

**Create new relationship registry**

| Field | Description |
|---|---|
| Name | A descriptive name for this registry. |
| Table | The table for which you want to define a relationship. |
| Relationship type | The type of relationship you are defining:<br>◦ One-to-many<br>◦ Many-to-many<br>◦ Scripted: a custom relationship from the Now Platform<br>◦ One-to-one: any relationship that is available as a field in the selected table |
| Active | Select if the relationship is active. |
| Relationship | The relationship table of the selected relationship type. For example, if you are defining relationships for the Entity table and select a many-to-many relationship type, the list of relationship tables consists of all many-to-many relationships that apply to the Entity table. |
| Relationship table | The table name you selected in the **Relationship** field. |

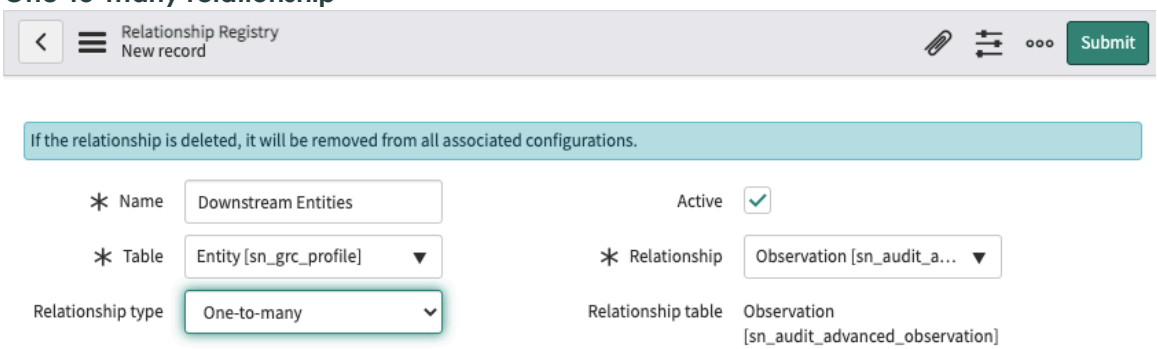
4. Click **Submit**.
5. Repeat this process for all of the relationships you want to appear in the 360° Relationship Visualization interface.

### 360° relationship examples

These screen shots illustrate the various relationship types you can register.

## One-to-many relationship

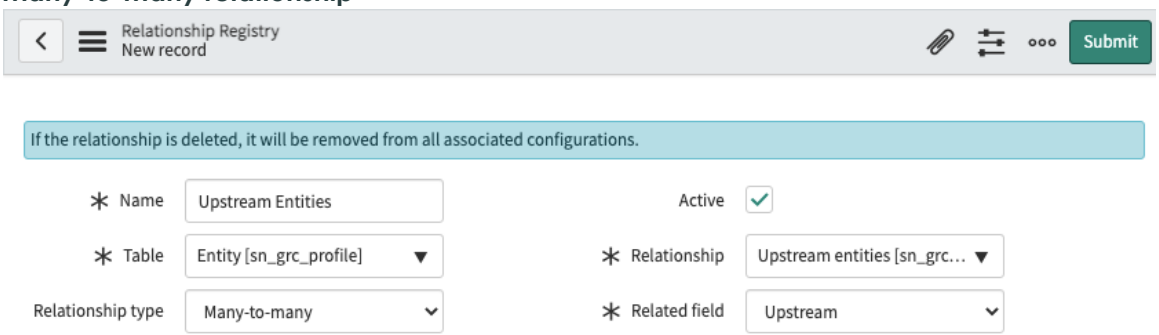
**One-to-many relationship**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

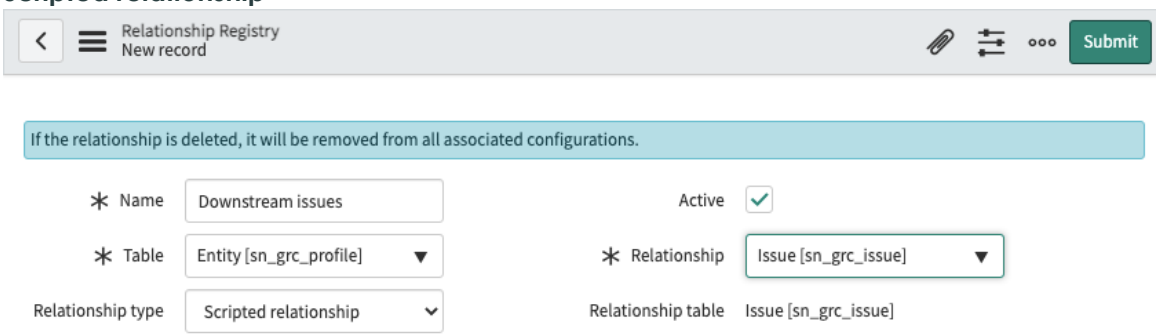
## Many-to-many relationship

### Many-to-many relationship



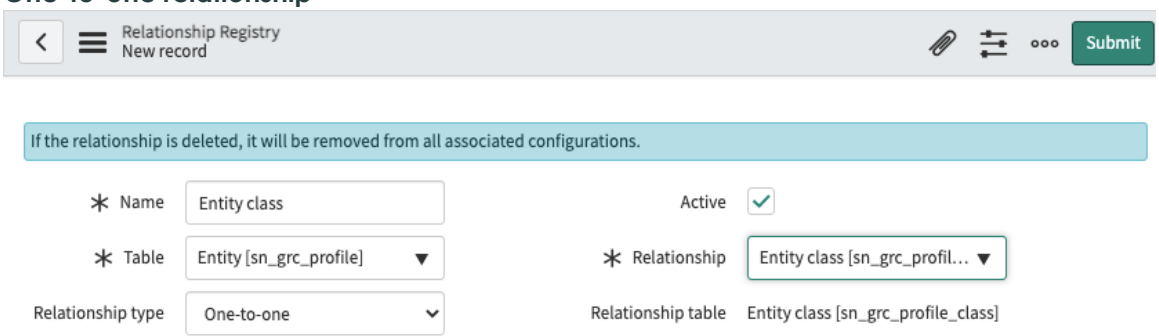

## Scripted relationship

### Scripted relationship




## One-to-one relationship

### One-to-one relationship




### Configure 360° views

After the data registry has been defined, you can configure the 360° Relationship Visualization to effectively display the relations you created.

**Before you begin**
Role required: Data registry administrator

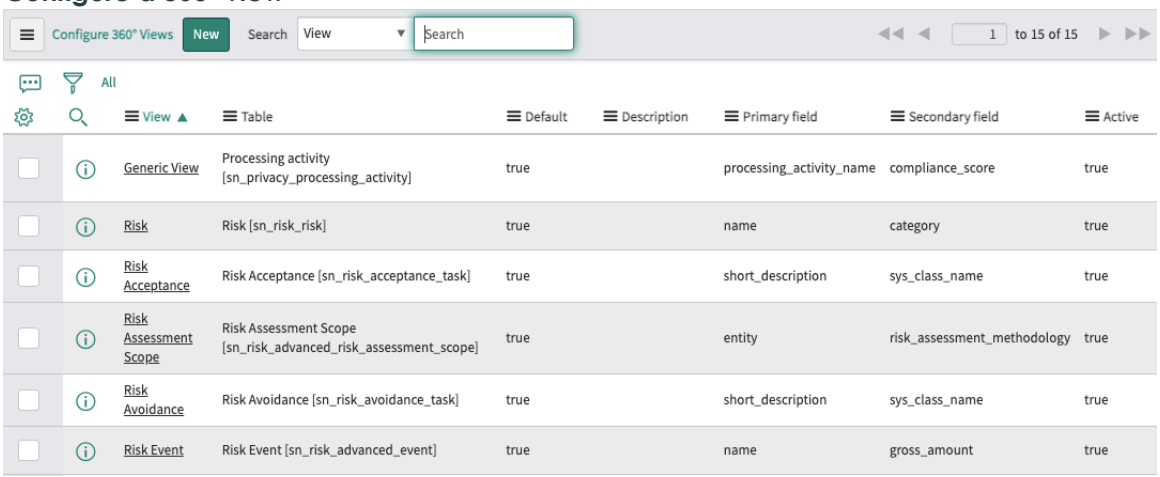
**About this task**
Multiple 360° Relationship views can be configured for a table. For example, the Entity table can be configured with multiple views, such as Compliance view, Risk view, Audit view, and others.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Procedure

1. Navigate to **360° View Configurations** > **Configure 360° Views**.

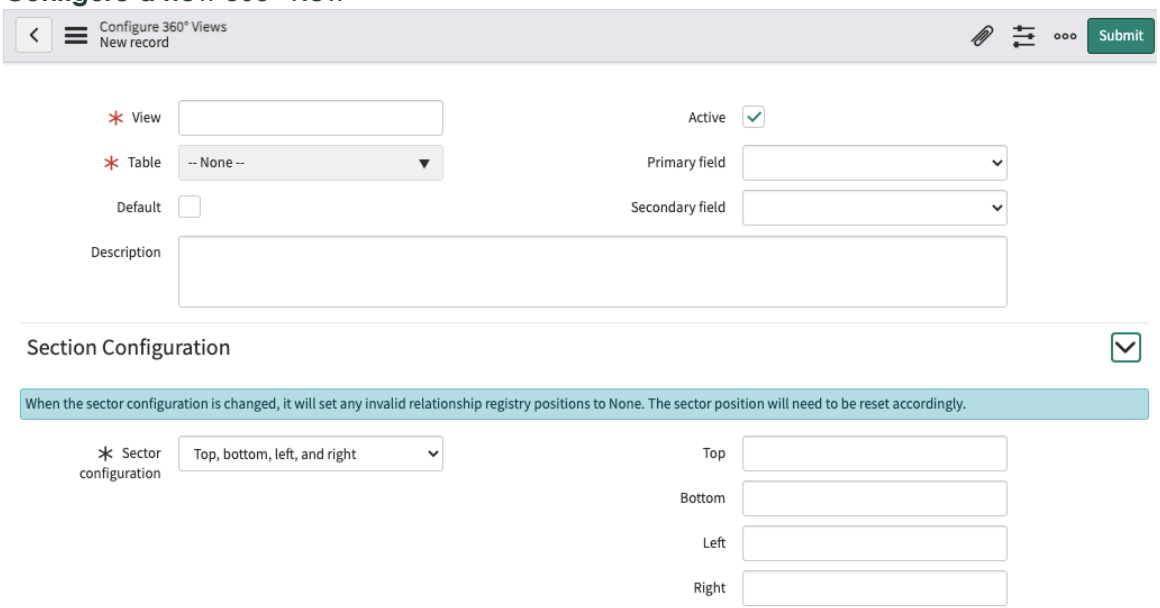
**Configure a 360° view**




| View | Table | Default | Description | Primary field | Secondary field | Active |
|---|---|---|---|---|---|---|
| Generic View | Processing activity [sn_privacy_processing_activity] | true | | processing_activity_name | compliance_score | true |
| Risk | Risk [sn_risk_risk] | true | | name | category | true |
| Risk Acceptance | Risk Acceptance [sn_risk_acceptance_task] | true | | short_description | sys_class_name | true |
| Risk Assessment Scope | Risk Assessment Scope [sn_risk_advanced_risk_assessment_scope] | true | | entity | risk_assessment_methodology | true |
| Risk Avoidance | Risk Avoidance [sn_risk_avoidance_task] | true | | short_description | sys_class_name | true |
| Risk Event | Risk Event [sn_risk_advanced_event] | true | | name | gross_amount | true |

2. Click **New**.

**Configure a new 360° view**

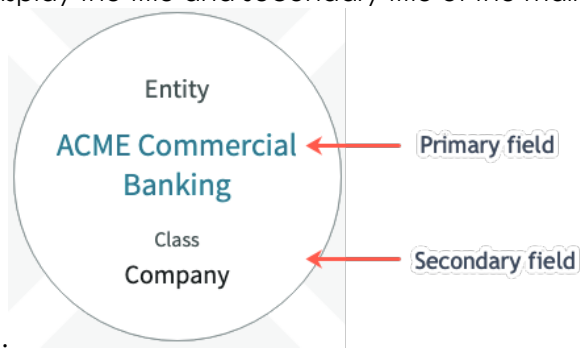



3. On the form, fill in the fields.

**Create 360° view**

| Field | Description |
|---|---|
| View | A descriptive name for this view. |
| Table | The table for which you want to define the view. |
| Default | Select if this is the first view you are defining or your only view. |
| Active | Select if this 360° view is active. |

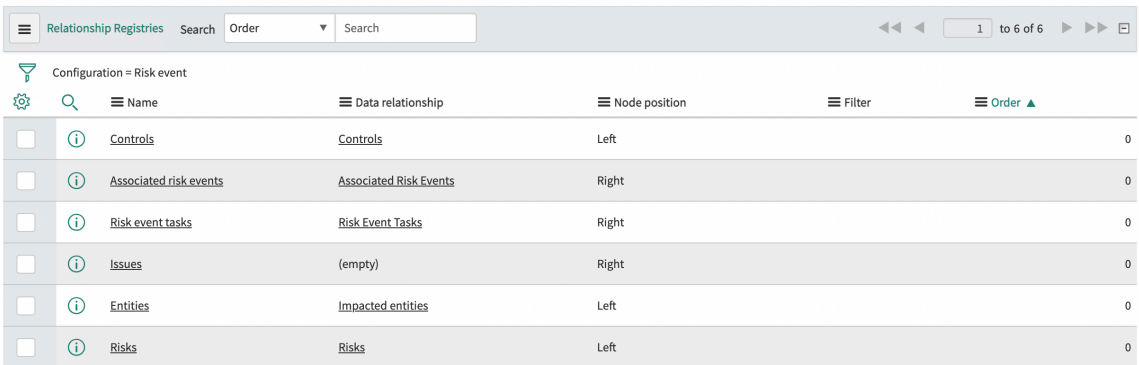
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Primary field and secondary field | The primary and secondary fields in the selected table to be used to display the title and secondary title of the main object, as   illustrated. |
| Description | A description of the 360° view. |
| Section Configuration | |
| Sector configuration | Select the number of sectors to be displayed in the 360° view. For example, select `top, bottom, left, and right` to indicate you want four sectors. |
| Top, Bottom, Left, Right | Based on your **Sector configuration** selection, enter labels for each of the sectors. |

4. Save the record.

   The Relationship Registries related list appears.

### Relationship registries




5. Click **Select Relationships**.
6. On the form, fill in the fields.

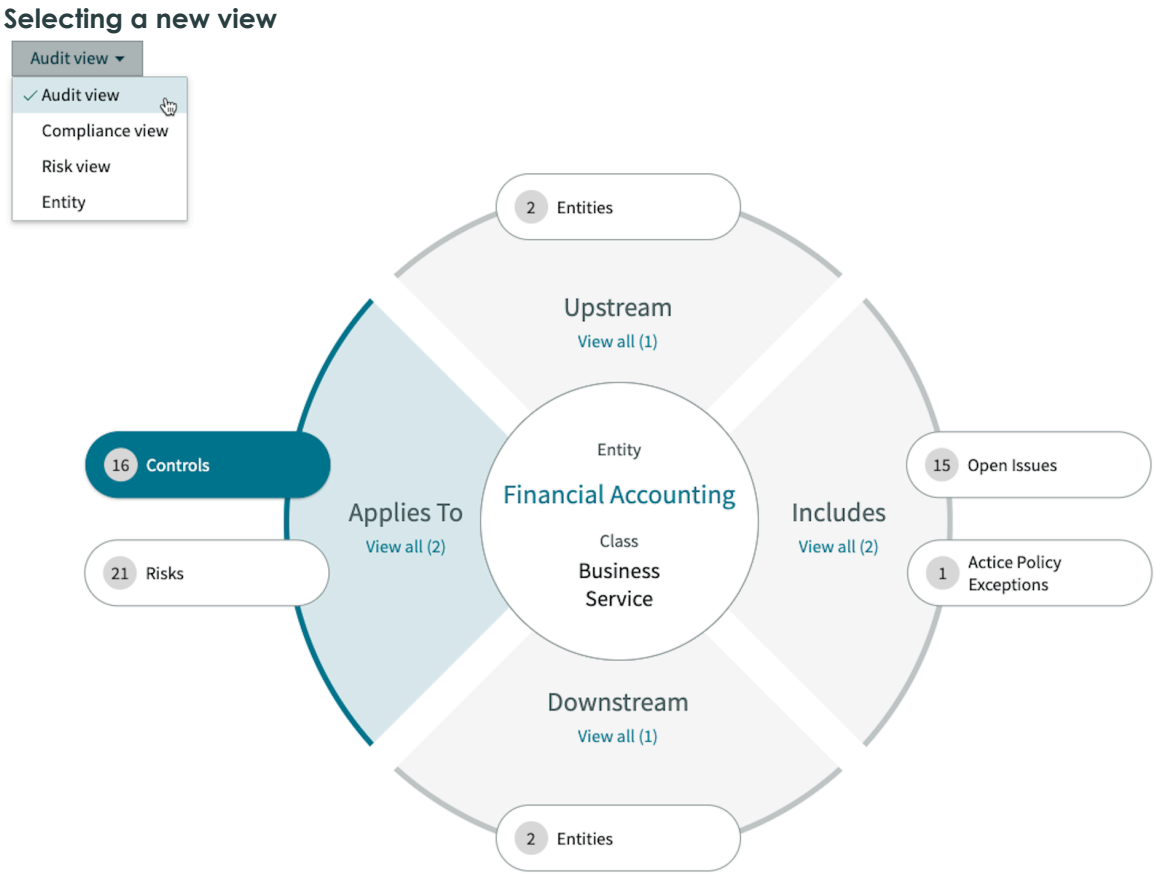
### DataNav Config to Data Relationship

| Field | Description |
|---|---|
| Name | A name to identify this relationship. |
| Data relationship | The data relationship you previously defined. |
| Relationship table | The table associated with the selected data relationship. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Node position | The sector you previously defined to which you want to add this relationship. |
| Filter | Enter conditions to define the types of relationships you want to display. For example, you could define conditions for all controls with failures. |
| Configuration | The configuration defined for the relationship. |
| Table | The table defined for the relationship. |
| Order | Based on the **Order** value given the position of element in the 360° view will change.<br><br>For example, if you change the order value from 0 to 1 for an element, the position will be moved to next in the 360°view. |

7. Click **Submit**.
   The new view you have defined is now available on the 360° view.




## Exploring the 360° view

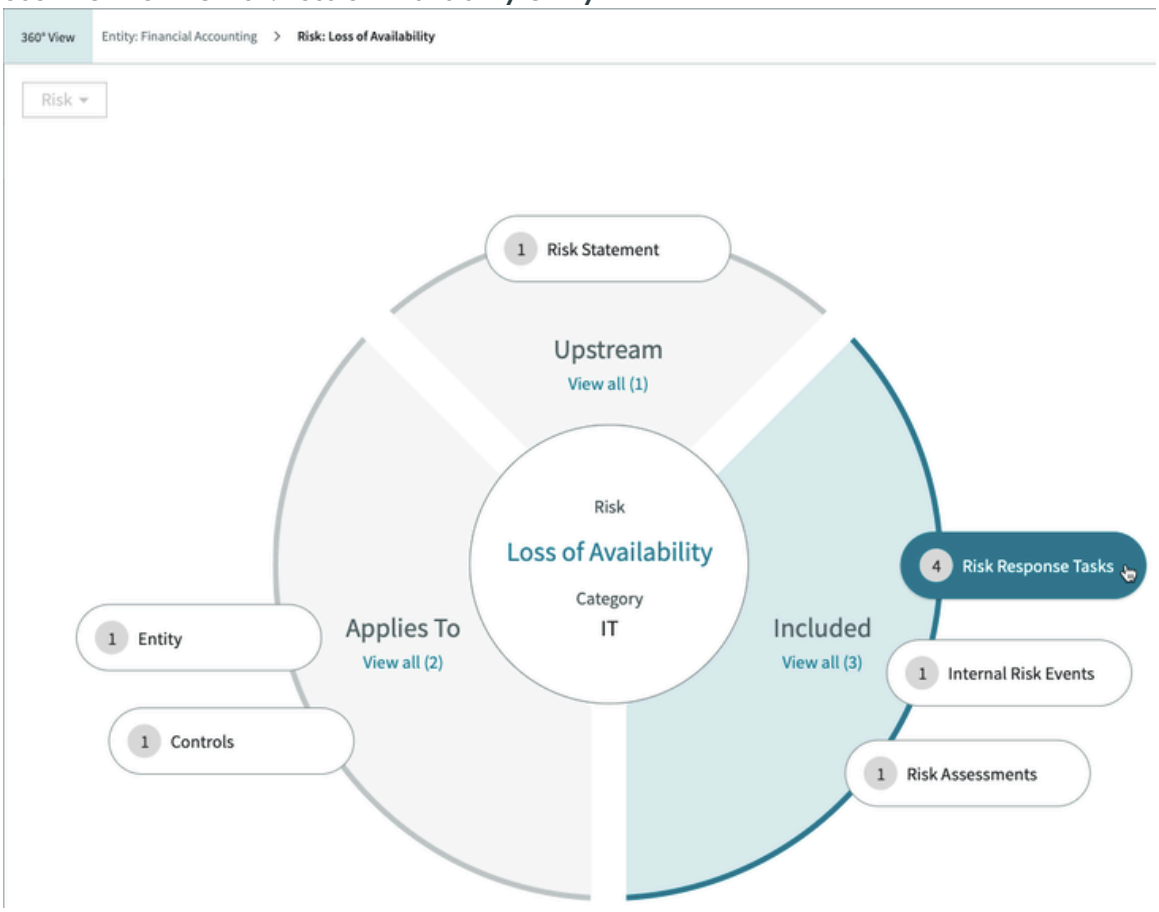
After you have successfully set up your data registries for the tables you use, you can use the 360° view feature to view the relationships between a selected record and related objects, such as controls, risks, and entity types.

When you launch the 360° view from a particular record, the relationships between the selected record and all associated objects are displayed in a distinctive visualization that allows you to instantly understand how the objects interact with one another. The

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

relationships are linked to your data so you can perform actions on the displayed records, such as drilling down into them to view additional details or creating new records.

**360° view for the Risk: Loss of Availability entity**




The screen above shows the relationships that you set up in the data registry for the selected main object (in this case, the Risk: Loss of Availability entity). As you can see, one entity and one control apply to the main object. And the main object includes a range of relationships related to risk response tasks, internal risk events, and risk assessments. Additionally, there is a risk statement relationship upstream from the main object. All these relationships to the main object are available to you at a glance.

### Launch the 360° view

After data registries have been set up, you can launch 360° view from any record screen in any GRC workspace application to view relationships between the various types of data associated with the selected record.

### Before you begin

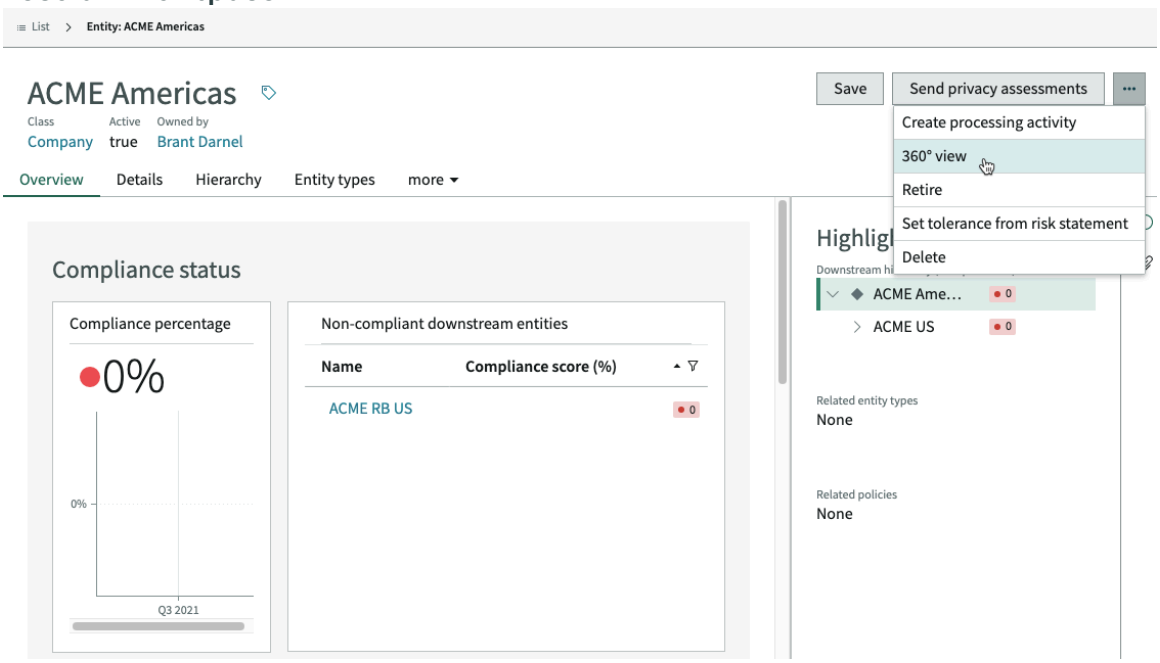
Role required: data registry reader

### Procedure

1. Navigate to any GRC workspace, for example the Compliance Workspace.
2. Open a record for which you want to open in the 360° view.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Record in workspace**

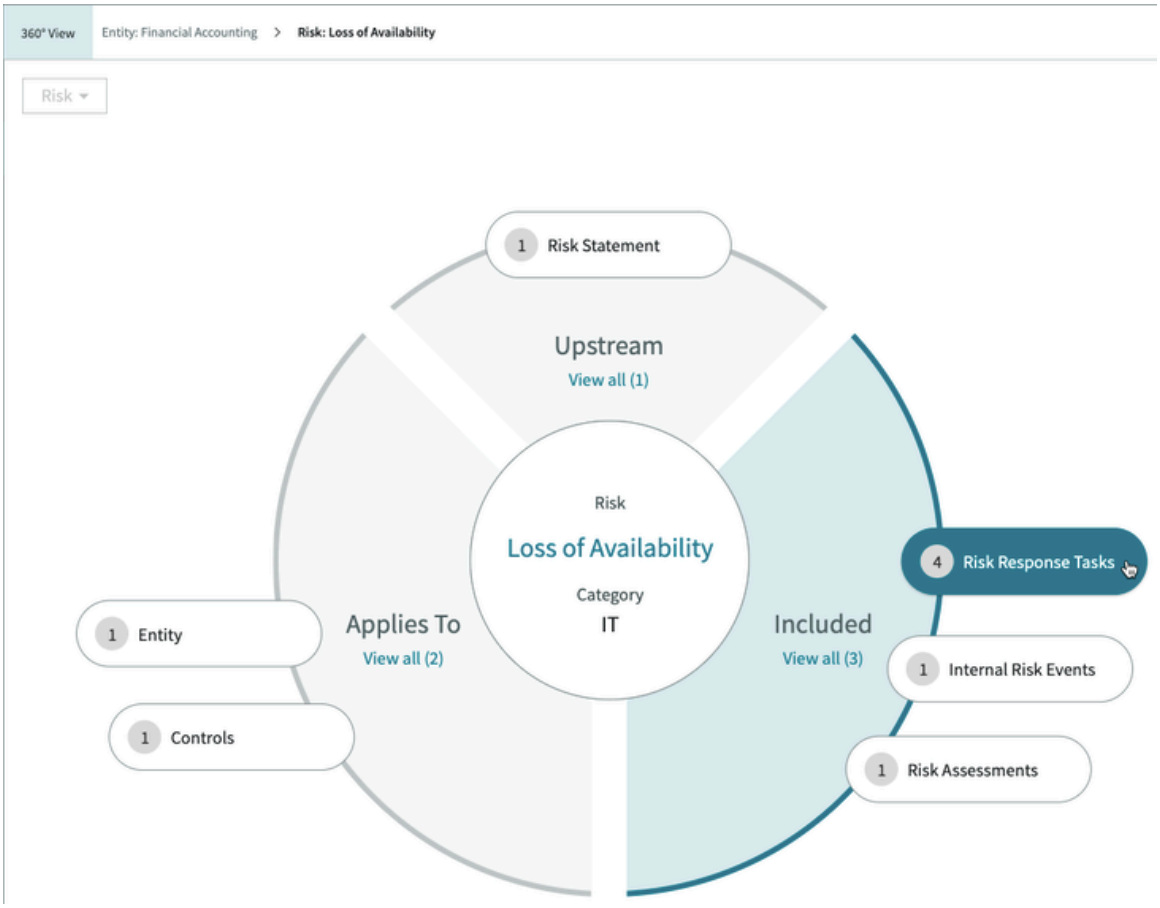



**Note:** Depending on the record screen, you may need to click the ellipsis icon to view the **360° view** button.

3. Click **360° view**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### 360° view of selected record




**Note:** If you launch the 360° view prior to configuring your data registries, or if you click on an object within the 360° view that has not been configured, the visualization screen opens in fallback (or unconfigured) mode. All one-to-many and many-to-many relationships for the object are automatically calculated and displayed in the view.

A system property called `sn_data_registry.max_count_of_fallback_relationships` allows you to define the maximum number of relationships to display in the 360° view. The default is 25.

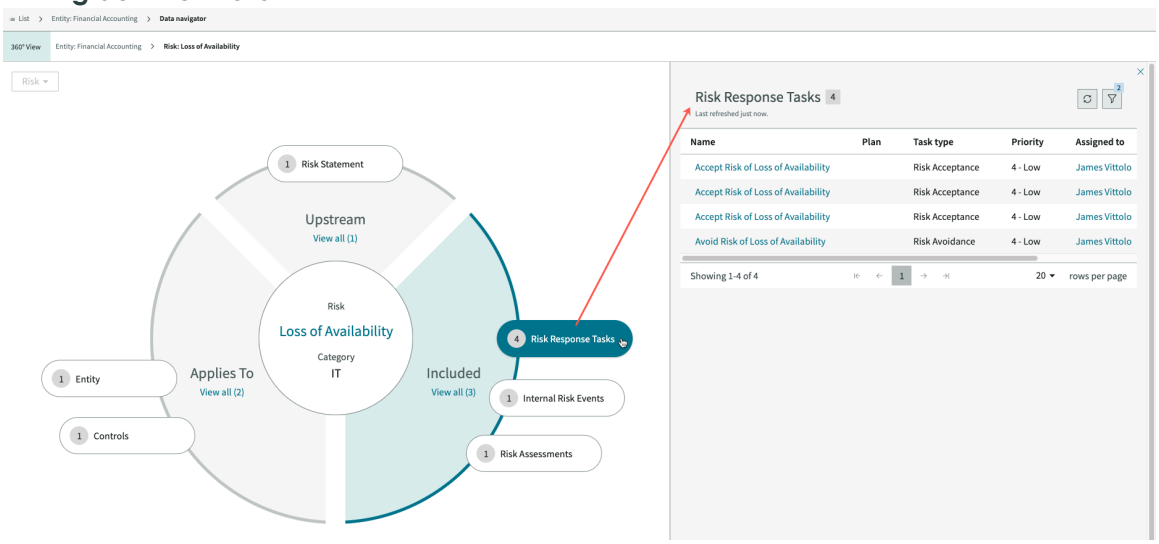
### Drilling-down for 360° details

In the 360° view, you can click on any relationship to view details.

For example, you can click on the **Risks** relationship to view details on four risks.

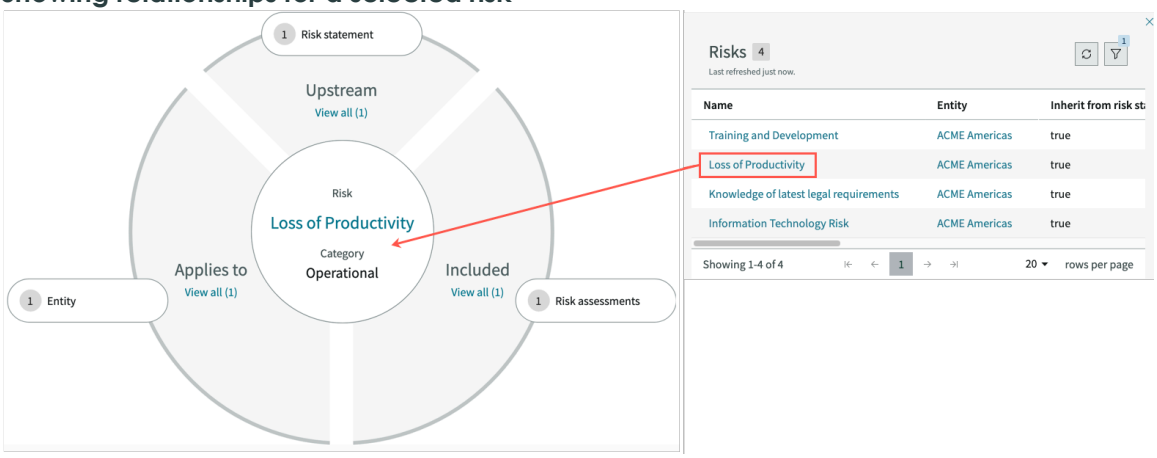
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Drilling down on risks




You can then select one of the risk records to view relationships specific to that risk record.

### Showing relationships for a selected risk




## Navigating the 360° view using breadcrumbs

As you navigate through 360° view relationship visualizations, the breadcrumbs along the top edge keep track of where you've been and allow you to return to previously viewed information.

### 360° view breadcrumbs

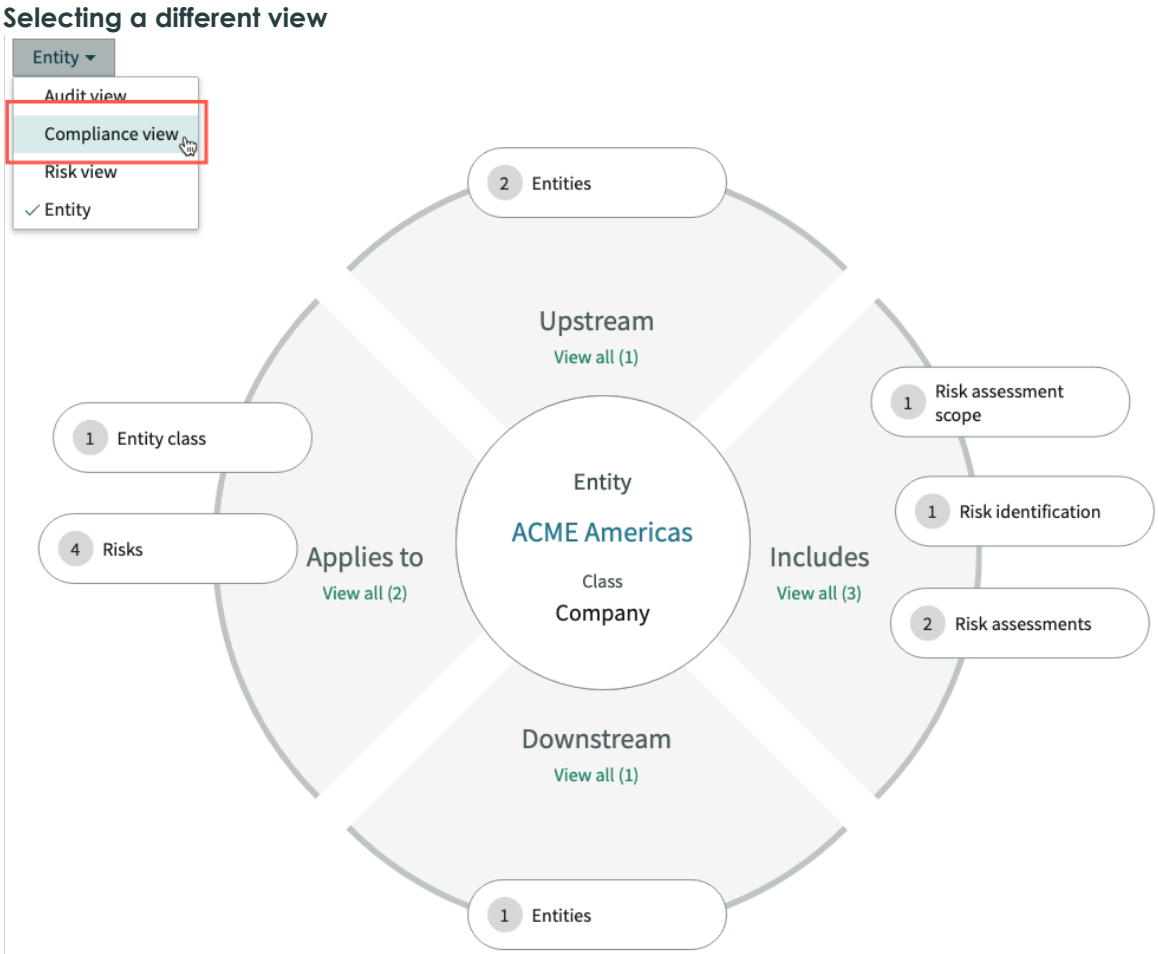



Clicking the **Entity: ACME Americas** breadcrumb returns you to a visualization of those relationships.

## Selecting different 360° views

If you have defined different views, you can select them from any 360° view visualization.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




The Compliance view presents you with relationships for the main object that are specific to compliance, as you configured it.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




Related topics

Configure 360° views

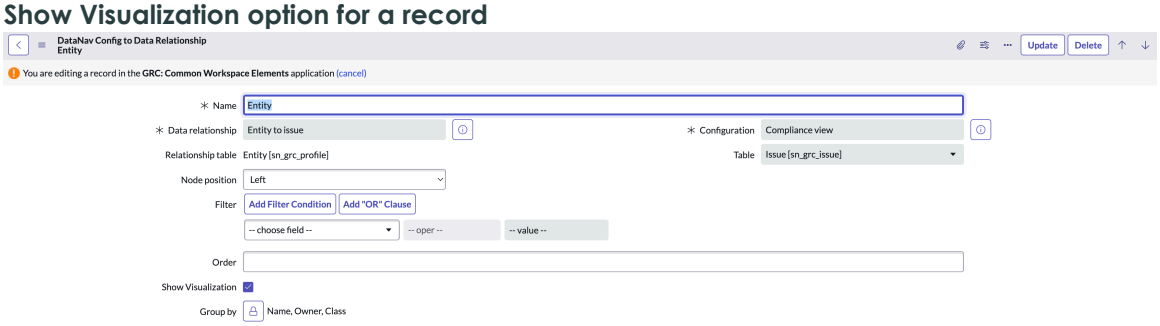
### Enhancements in the 360° view

You can configure some functionality enhancements for the 360° view of each record as part of the GRC updates.

The following enhancements and bug fixes are supported with the updated 360° view:

- Displaying an interactive donut chart: You can enable the **Show Visualization** option for each record and select the display columns in the **Group by** list. See the following example.

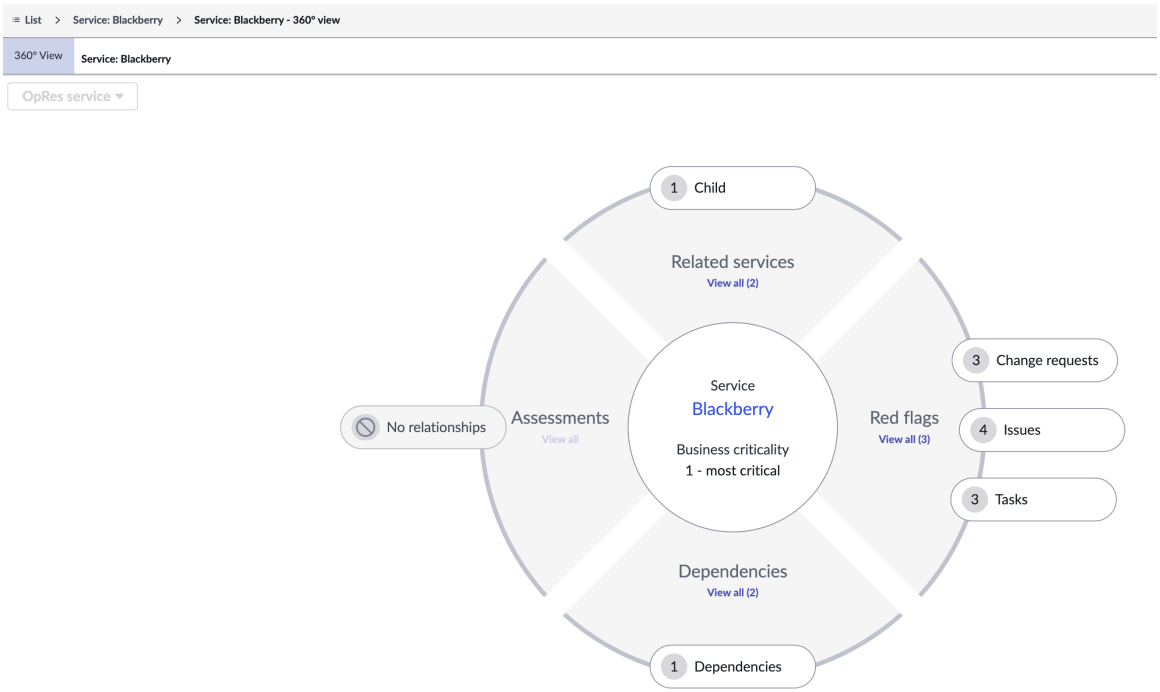
**Show Visualization option for a record**




When you enable the **Show Visualization** option for a record, the 360° view is displayed. In the 360° view, you can view all the objects that are associated with the record as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

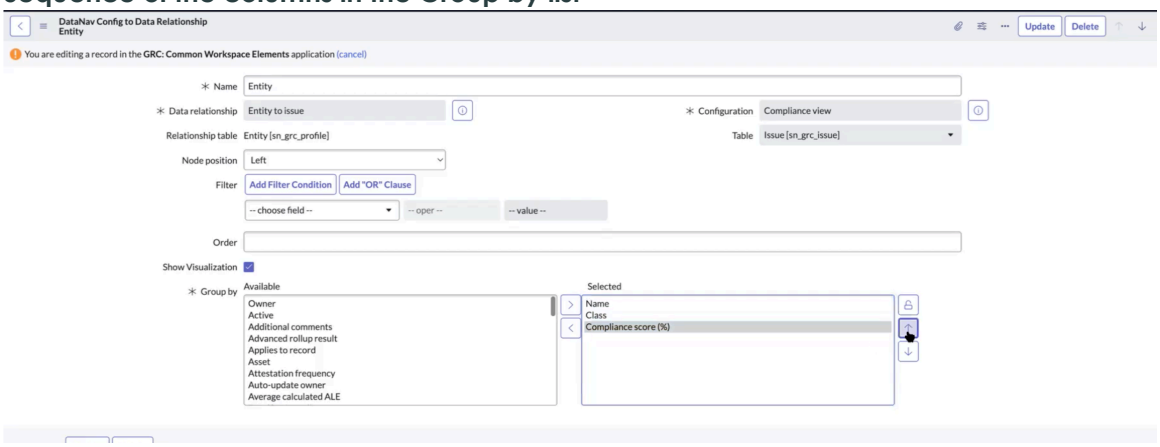
### 360° view for a record




When you click any sector of the donut chart, the related lists that are associated with the selected object are refreshed. When you click an object pill, it displays the donut chart for the selected object in the side-panel.

- Configuring the Group by list: You can configure the number and order of the columns in the Group by list. When you update the columns in the Group by list as shown in the following example, the donut chart is refreshed for the selected columns.

### Sequence of the columns in the Group by list




When you select a specific order of the columns in the Group by list, the same order of the columns is reflected in the UI. The first column that is displayed in the Selected list is the default value in the display for the customers.

- Order of the pills: You can configure the order of the pills for each section in the **Order** field. If you have not configured the order of the pills and all the pills have the same order value (for example, if each pill has an order value of 1), the pills appear alphabetically.
- The defect fixes are as follows:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Defect fix on the related lists: A defect on the related lists was fixed. A new sys_relationship field was added in the code to avoid a conflict among the related lists that refer to the same table.
- Defect fix for the Apple iPad Pro devices: Earlier, multiple vertical and horizontal scrolls were displayed in the default view on the smaller Apple iPad devices such as the 12.9-inch (0.328 meter) and 16-inch (0.406 meter) Apple iPad Pro devices. The defect related to the view on the smaller Apple iPad devices has been fixed. You can see the entire 360° component on an Apple iPad device without needing to scroll the view.
- Defect fix on the navigation path: A defect that is related to the caching issue that existed in the prior releases was fixed. You can now view the navigation path correctly for the records.

## Using the item generation process to generate controls and risks

The ServiceNow® GRC suite of applications can automatically generate controls and risks for your organization with the enhanced item generation process. The enhanced item generation process (v2) in version 13.x.x fixes the stalling and performance issues from the item generation process (v1) in version 12.x.x and earlier releases.

### Overview of the item generation process

By using the Governance, Risk, and Compliance application, you can use the item generation process to generate controls and risks for your organization.

A control is the actual control activity that an organization performs. For example, a control can be related to authoritative source content (legal articles, regulations, or public records), policies, and risks. A control is automatically generated when you associate a policy with an entity type (grouping of the entities that match a set of filter conditions) or an entity type with a control objective. For more information on controls, see Manage controls .

A risk is any threat or vulnerability that could adversely affect an organization's business objectives. For example, a risk can be related to any item, policy, control, or remediation task. A risk is automatically generated when you make associations between risk frameworks or risk statements and entity types.

**Note:** Risk statements are general statements about potential risks or threats that could occur in an organization. A risk framework consists of a risk assessment, response, and accountability for the risk and mitigation activities around it.

For more information on risks, see Using Risk Management .

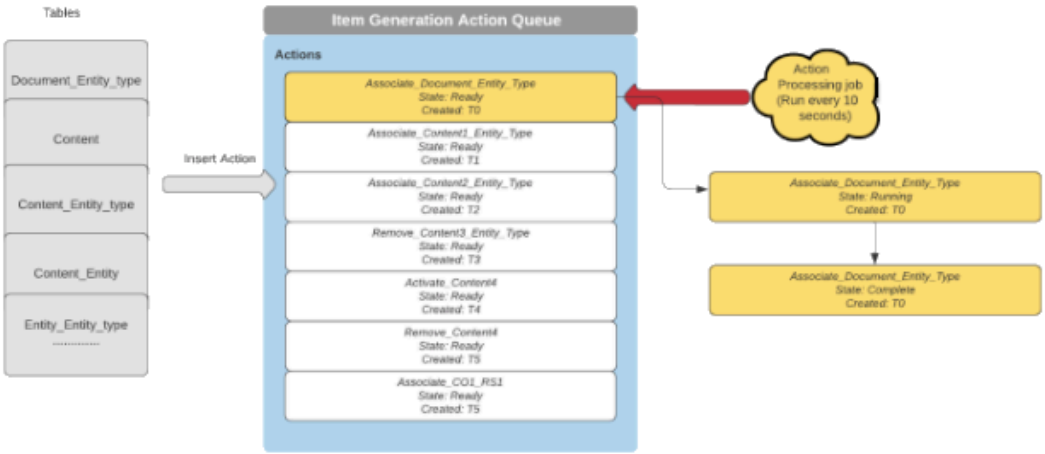
The item generation process (v1) in version 12.x.x and earlier releases generated out-of-sync updates due to the stalled actions in the action queue. The enhanced item generation process (v2) eliminates the stalling issues and improves the processing time of the controls and risks significantly. For example, the legacy item generation process (v1) generated 10,000 risks in approximately 13.7 minutes where the new item generation process (v2) can generate 10,000 risks in approximately 5.27 minutes.

### Flow of the item generation process

The item generation process inserts an action in the action queue and executes the actions one by one in a sequence. A scheduled job runs periodically to check the action queue. If an action is running in the queue, the scheduled job skips it. When the current running action is completed and no other action is in process, the scheduled job picks up the next action in the Ready state in the queue as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Item generation process flow




## Benefits of the item generation process

The new item generation process provides the following key benefits:

- Processes the controls and risks quickly by using the item generation action event queue.
- Eliminates the stalled actions and race conditions in the queue that generated the non-consistent updates.
- Logs the history and status of the item generation actions.
- Provides more information about an error in the item generation action event queue. It helps you to track and troubleshoot the issues quickly and efficiently.
- Helps the compliance and risk managers to manage the controls and risks in an auto-pilot mode without much maintenance.

## Applications that are used in the item generation process

The following GRC applications are used in the item generation process:

- GRC: Policy and Compliance Management
- GRC: Risk Management
- GRC: Profiles

The GRC: Profiles application is automatically installed when either the GRC: Policy and Compliance Management or GRC: Risk Management application is activated.

## Upgrade scenarios and their impact on the existing implementations

You must upgrade both Policy and Compliance Management and Risk Management applications to version 13.x.x. When you upgrade the Policy and Compliance Management and Risk Management applications to version 13.x.x, the new item generation process (v2) replaces the legacy item generation process (v1).

**Note:** Upgrading the Policy and Compliance Management and Risk Management applications to version 13.x.x automatically upgrades the GRC: Profiles application to version 13.x.x.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Ensure that you have the required versions of the Policy and Compliance Management and Risk Management applications installed in your instance. If you have one of the following scenarios for the installed applications, you receive an error message on the screen:

- You have both the Policy and Compliance Management and Risk Management applications previously installed in your instance and you upgrade only one of them to version 13.x.x.
- You have only one of the Policy and Compliance Management or Risk Management applications installed in your instance and you upgrade the GRC: Profiles application to version 13.x.x.
- You have both Policy and Compliance Management or Risk Management applications installed in your instance and you upgrade the GRC: Profiles application to version 13.x.x.

The error message states that you must upgrade both Policy and Compliance Management and Risk Management applications to version 13.x.x as shown in the following example.

**Message for upgrading the applications**




When you upgrade, you don't see any visible impact to your existing implementations of the item generation process.

**Note:** If you haven't upgraded to version 13.x.x, the legacy item generation process is still supported.

## Components that are used by the item generation process

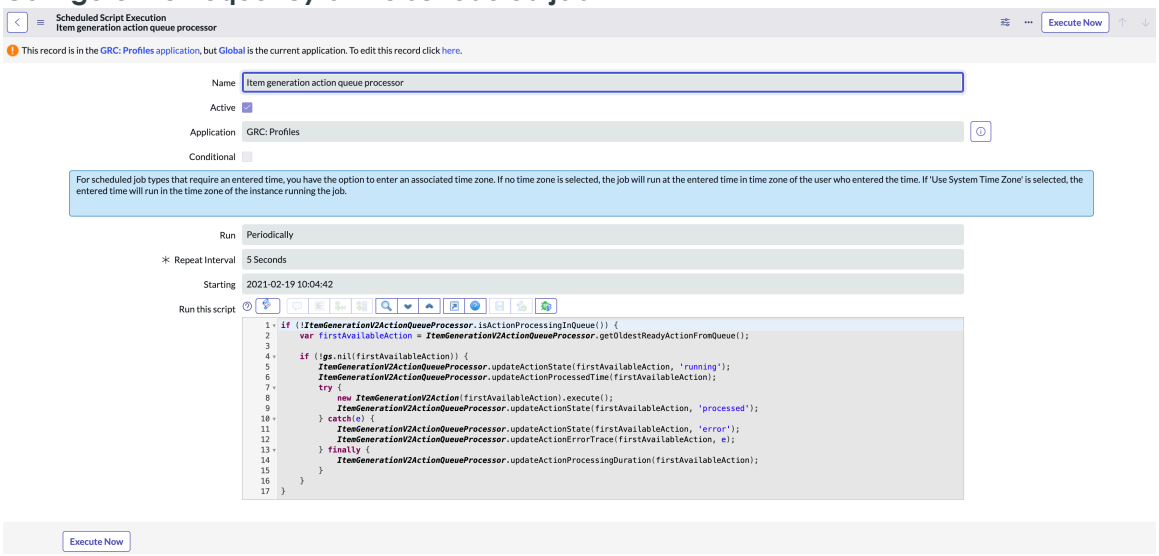
The item generation process uses several types of reference components such as tables, scheduled jobs, and action handlers. For more information on the components that are used with the item generation process, see Components installed with the item generation process.

## Using the scheduled job and action event queue

The item generation process uses the *Item generation action queue processor* scheduled job and an action event queue in the background. As a user with the sn_grc.admin role, you can configure the frequency of the scheduled job as shown in the following example.

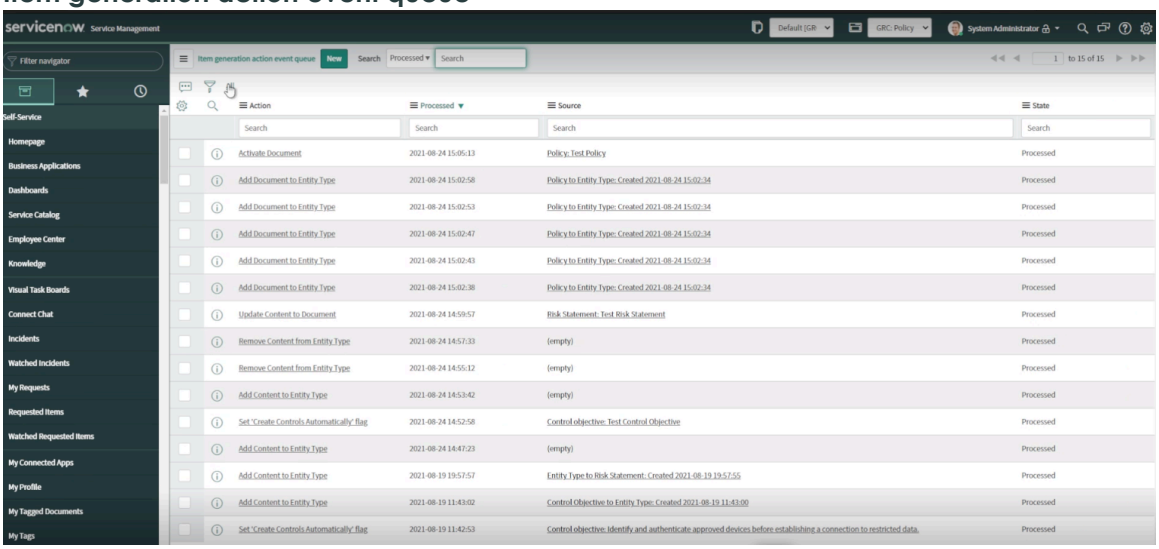
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Configure the frequency of the scheduled job




When you initiate an action that results in generating, updating, or deleting a control or risk, the scheduled job inserts a record for each action in the sn_grc_item_generation_action_event_queue.list table. The item generation action event queue is shown in the following example.

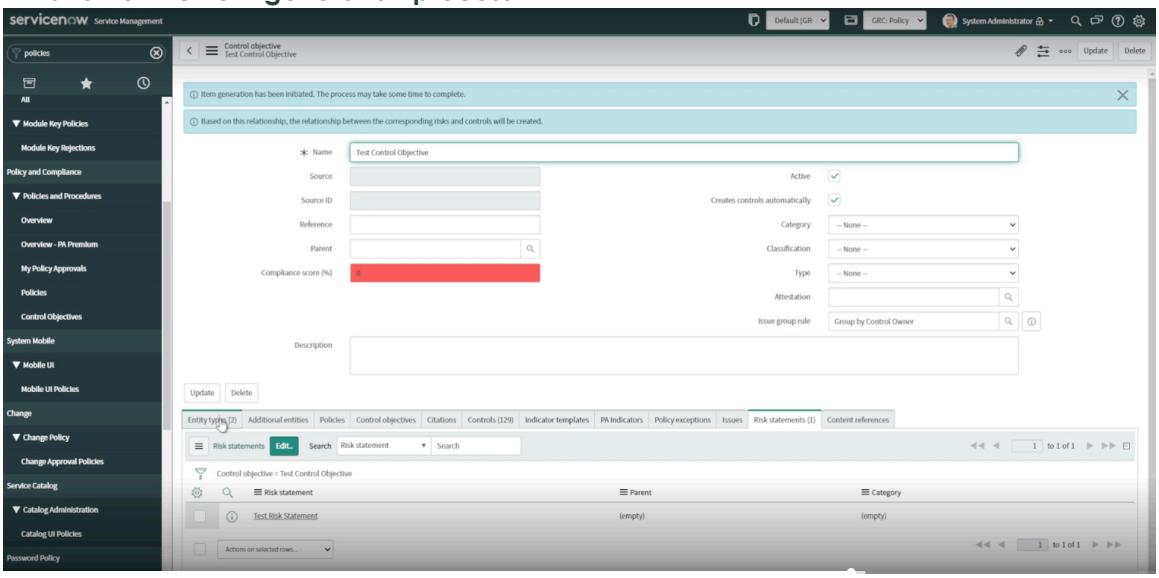
### Item generation action event queue




When an action is generated by using the item generation process, a message that the item generation process has been initiated is displayed. For example, when you add a risk statement to a control objective, you see the message that is shown in the following example.

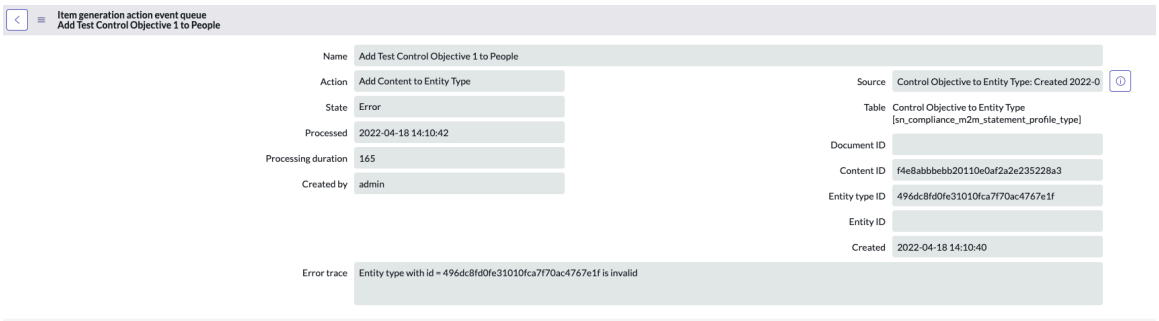
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Initiation of the item generation process




If an error occurs while processing an action in the queue, the item generation process displays more information about the error. For example, you might see an error trace with the object ID as shown in the following example.

### Error trace




You can use the error trace and other details in the queue to track and troubleshoot the issue.

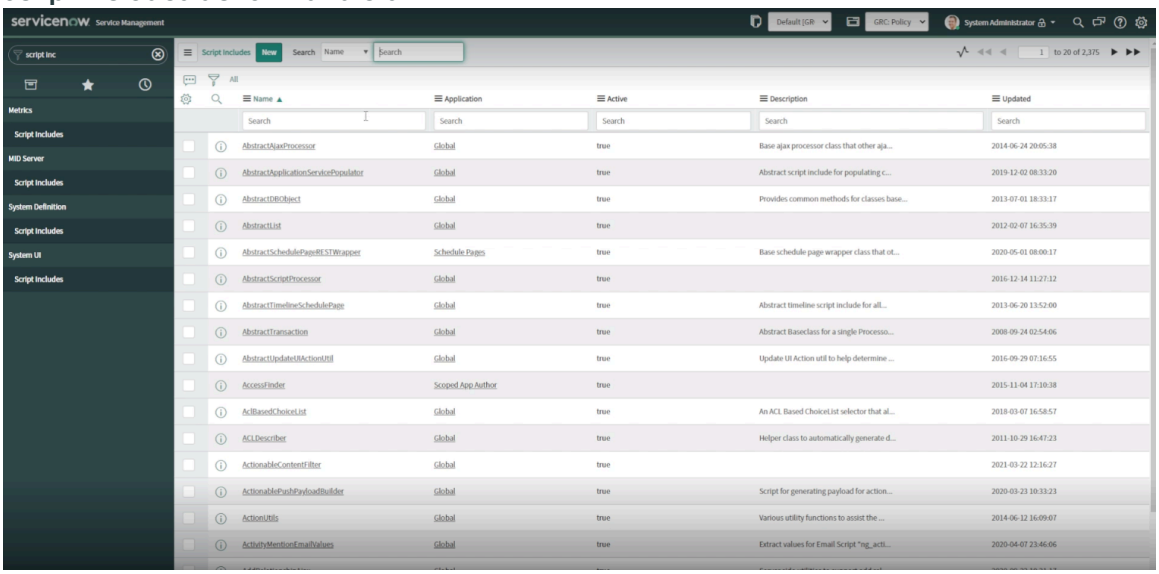
## Script includes action handlers

The item generation process uses the script includes action handlers that process the actions for the Policy and Compliance Management and Risk Management applications.

You can view the list of the supported action handlers by navigating to **Script Includes** in the application navigator as shown in the following example.

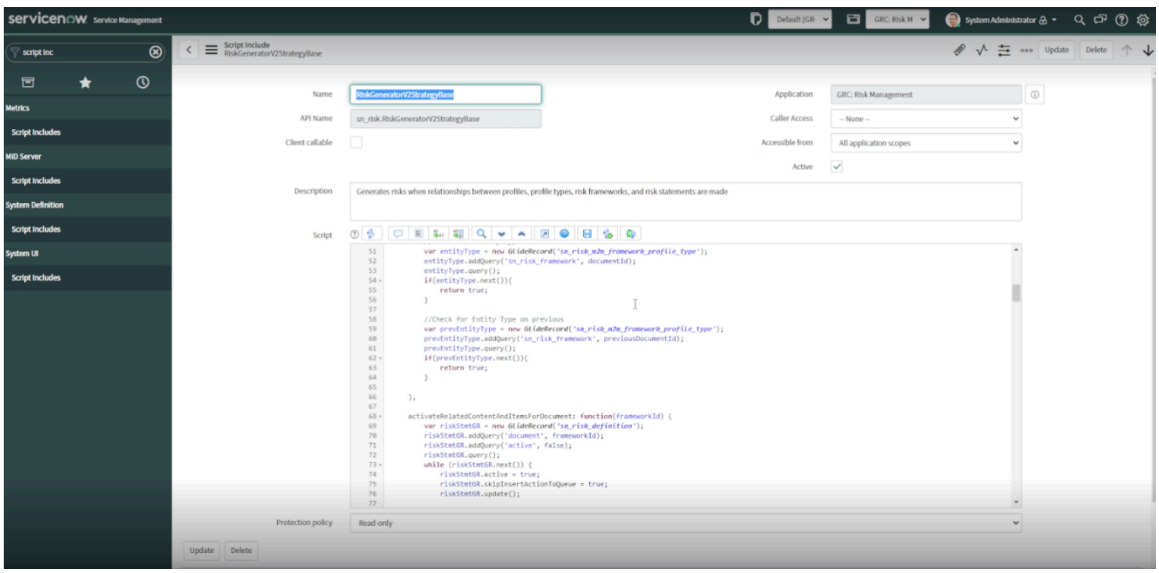
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Script includes action handlers




All script includes action handlers contain the base version and the extended version. The item generation process uses the base version for handling the actions. As a user with the sn_grc.manager role, you can review the base functions that are listed in the action handler as shown in the following example.

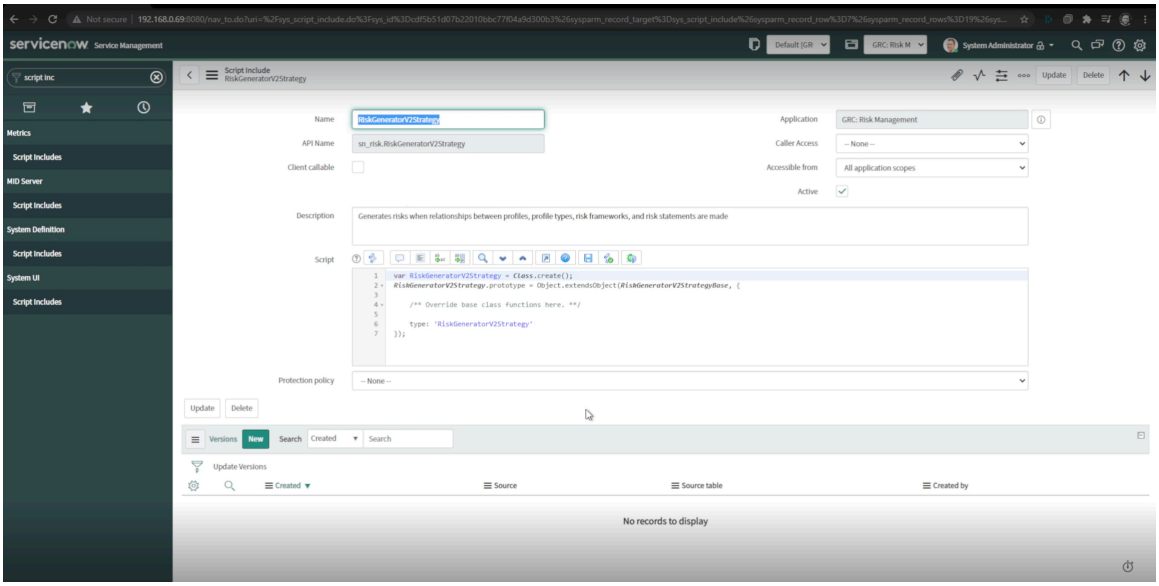
### Base functions




As a user with the script_include_admin role, you can revise the action strategy for a control or risk by overriding the base functions as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Override the base functions




## Components installed with the item generation process

Several types of components are installed with the item generation process, including tables, scheduled jobs, and action handlers.

The following components are installed with the item generation process in version 13.x.x.

### Components that are installed with the item generation process

| Component | Description |
|---|---|
| Table | |
| Item Generation Action Event Queue table (sn_grc_item_generation_action_event_queue) | Table that lists the actions that are generated during the item generation process. |
| Scheduled job | |
| Item generation action queue processor | Scheduled job to process the action queue. The job runs every five seconds by default. |
| Action handlers | |
| ItemGenerationV2Action | Single view of all the action handlers that are used for item generation. |
| IGContentToEntityTypeActionHandler | Handler to be called when you perform one of the following actions:<br>• Add control objectives and risk statements to the entity type.<br>• Remove control objectives and risk statements from the entity type. |
| IGDocumentToEntityTypeActionHandler | Handler to be called when you perform one of the following actions: |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Components that are installed with the item generation process (continued)**

| Component | Description |
|---|---|
| | • Add policies and risk frameworks to an entity type.<br>• Remove policies and risk frameworks from an entity type. |
| IGEntityTypeActionHandler | Handler to be called when you perform one of the following actions:<br>• Activate entity type.<br>• Delete entity type.<br>• Deactivate entity type. |
| IGEntityToEntityTypeActionHandler | Handler to be called when you perform one of the following actions:<br>• Add an entity to an entity type.<br>• Remove an entity from an entity type. |
| IGContentActionHandler | Handler to be called when you perform one of the following actions:<br>• Activate control objectives and risk statements.<br>• Deactivate control objectives and risk statements.<br>• Create control objectives and risk statements.<br>• Set an auto-control create flag.<br>• Add control objectives to risk statements.<br>• Remove control objectives from risk statements.<br>• Delete control objectives and risk statements. |
| IGDocumentActionHandler | Handler to be called when you perform one of the following actions:<br>• Activate policies and risk frameworks.<br>• Deactivate policies and risk frameworks.<br>• Add control objectives and risk statements to policies and risk frameworks.<br>• Delete control objectives and risk statements from policies and risk frameworks. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Components that are installed with the item generation process (continued)**

| Component | Description |
|---|---|
| IGEntityActionHandler | Handler to be called when you perform one of the following actions:<br>• Activate an entity.<br>• Deactivate an entity. |
| IGContentToAddtlEntityActionHandler | Handler to be called when you perform one of the following actions:<br>• Add control objectives and risk statements to an additional entity.<br>• Remove control objectives and risk statements from an additional entity. |
| IGItemActionHandler | Handler to be called when you perform one of the following actions:<br>• Activate an item.<br>• Deactivate an item.<br>• Delete an item. |
| IGItemToEntityActionHandler | Handler to be called when you perform one of the following actions:<br>• Add entity to item.<br>• Activate entity to item.<br>• Remove entity from item.<br>• Deactivate entity to item. |
| IGItemToEntityTypeActionHandler | Handler to be called when you perform one of the following actions:<br>• Add entity type to item.<br>• Remove entity type from item. |

**Note:** For more information on the item generation process for common controls, see the new action types in generation of items.

## Roles and users for the new item generation process

Users with the sn_grc.admin or sn_risk.manager role role can access the sn_grc_item_generation_action_event_queue.list table in an instance and view the item generation action queue.

The compliance and risk user roles and their associated tasks that trigger the item generation process are listed in the following table.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** The compliance and risk user roles that are listed in the table are available with version 12.x.x and earlier releases.

### Compliance and risk user roles and their associated tasks

| Compliance and risk user roles | Associated tasks |
|---|---|
| • sn_compliance.admin<br>• sn_risk.admin | • Delete policies.<br>• Delete risk frameworks.<br>• Delete control objectives and risk statements.<br>• Delete an entity.<br>• Delete an entity type. |
| • sn_compliance.manager<br>• sn_risk.manager | • Associate policies or risk frameworks to an entity.<br>• Delete policies or risk frameworks from an entity.<br>• Associate policies or risk frameworks to an entity type.<br>• Delete policies or risk frameworks from an entity type.<br>• Activate an entity type.<br>• Deactivate an entity type.<br>• Associate an entity to an entity type.<br>• Delete an entity from an entity type.<br>• Add control objectives to a risk statement.<br>• Delete control objectives from a risk statement. |
| • sn_compliance.manager<br>• sn_risk.manager<br>• Entity owner | • Activate an entity.<br>• Deactivate an entity. |
| • sn_compliance.user<br>• sn_risk.user | • Create control objectives and risk statements.<br>• Enable the **Creates controls automatically** option. |
| sn_risk.manager | • Add risk statements to a risk framework.<br>• Modify risk statements that are added to a risk framework. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Operational changes in item generation of common controls

Operational changes are made in item generation mainly because item generation either creates a control or activates an existing standard control. When it comes to associating a control to an entity, then associating a reliant entity to a common control takes precedence over creating a control for that entity.

## Creation of controls

If the existing controls in your system can be used for testing entities, then you can take advantage of the existing data and avoid creating controls. Having many controls can lead to control explosion. If that is not feasible, then you can associate a primary entity with a common control, test the common control, and implement the test results on the reliant entities of the common control. If both these options don't work, then you can create a control.

To create a common control, select **Common** in the **Function** field of the Control form. Select the **Convert to common** list UI action. A common control is created upon validation. It's mandatory that you select a control objective before you convert a standard control to common control.

## Association of reliant entities to common control

1. Use the Reliant entities related list in the Control form to add individual entities to the common control. You can also remove the reliant entities using the **Remove** button.
2. Use Reliant entity types related list in the Control form to add entity types to the common control. You can also remove the reliant entity types using the **Remove** button.
3. Use the **Inherit common controls** UI action in the Controls related list of the Risk form to select common controls grouped by control objectives.

**Note:** For more information on reliant entity associations for a common control, see Create a control using the Compliance Workspace and Convert standard control to common control and add reliant entities.

## Item generation – Assumptions

- There's no auto-generation of common controls.
- When the existence of common controls or associations of reliant entities to common control or standard controls are checked, the control's name, entity, and control objective must match.
- Order of precedence between standard and common controls:
  - If reliant association and standard control do not exist, then based on the action type, a standard control is created. Action types, for example can be Add content to entity type, Add document to entity type, Activate content, Activate document.
  - If reliant association and standard control do not exist, then based on the action type a reliant association to common control is created. Action type can be Add entity type to common control.
  - If the user's intent is not clear from the action type and a standard control does not already exist, then in conflicting entity type, the preference is to associate the reliant entity to the common control over creation of a standard control. Action type, for example can be Add entity to entity type.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Item generation changes

### New action types in the generation of items

| Item generation action type | Description |
|---|---|
| Add entity type to common control | If the entity is not associated with the common item, then the application associates the entity with the common item by creating an m2m association between the two. |
| Remove entity type from common control | If the entity is associated with the common item, and the Entity types field has other entity types or **Individually_added** is true in the m2m record, then the application removes the Entity type ID from the Entity types column or deletes the entity to common item m2m record. |
| Add entity to item | If Risk Management is installed, based on the risk statement associated to the control objective, the risk to common control m2m records are added in the Control to Entity m2m table after considering the reliant entities. |
| Remove entity from item | • If Risk Management is installed, based on the risk statement associated to the control objective, risk to common control m2m records are deleted in consideration of the reliant entities.<br>• If Privacy Management is installed, then the Processing Activity to common control m2m association based on its reliant entity and also the Processing Activity to control objective m2m association are removed. |
| Activate entity to item | If Risk Management is installed, based on the risk statement associated to the control objective, risk to common control m2m records are added in the Control to Entity m2m table in consideration of its reliant entities. |
| Deactivate entity to item | • If Risk Management is installed, based on the risk statement associated to the control objective, then the risk to common control m2m records are deleted after considering the control's reliant entities.<br>• If Privacy Management is installed and the Processing Activity corresponds to a reliant entity, then the Processing Activity |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**New action types in the generation of items (continued)**

| Item generation action type | Description |
|---|---|
| | to common control m2m association and also the Processing Activity to control objective m2m association are removed. |
| Activate item | A common item is added:<br>1. When no standard control exists with the same name, content (control and control objective), and entity combination.<br>2. If the entity is not reliant on any other common item with the same name, content, and entity.<br>3. When the entity is active.<br><br>A standard item is added:<br>1. Risk Management and Policy and Compliance Management plugins are installed<br>2. Based on the risk statement and control objective association, risks are associated to controls. |
| Deactivate item | • Common item: Deactivates all Control to Entity m2m records.<br>• Standard item: Deletes risks to control associations based on the Risk statement and Control objective associations. |

## Approval configuration

The Approver configurator application provides you with capabilities to define multiple levels of approvals based on the business rule definitions.

To set up multiple levels of approvals in your application, you must configure the following setup steps:

- Set up an approval configuration record. For more information, see Set up approval configuration.
- Set up the approval levels. For more information, see Set up approval levels.
- Set up the approval rules. For more information, see Set up approval rules.

**Note:**

For more information on the roles in the GRC: Approver Configurator application, see Roles installed with GRC: Approver Configurator.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Set up approval configuration

Set up approval configuration to enable multiple levels of approvals and select approvers for each level based on approval rules.

### Before you begin

You must install the GRC: Approver Configurator (sn_grc_appr) application for approval configurations.

Role required: sn_grc_appr.admin

### Procedure

1. Navigate to **All** > **Approval Configurator** > **Approval Configurations**.
2. Click **New**.
3. On the form, fill in the fields.

**Approval Configuration form**

| Field | Description |
|---|---|
| Name | Name of the approval configuration. |
| Applies to | Table from which a record is submitted for approval. For example, risk event, risk event reporting, business impact analysis, or any table. |
| Priority | Preference of approval configuration. |
| Filter condition | Condition applied on the table with reference to the **Applies to** field.<br><br>The approval configuration with higher priority that matches the filter condition for the business document is selected for approver evaluation. |
| Active | Option to enable the approval configuration as active. |

**Note:** You cannot have more than one approval configuration applying to the table with the same priority.

4. Click **Submit**.

## Set up approval levels

Assign multiple levels of approvals to users or groups to support each step of workflow processes.

### Before you begin

Role required: sn_grc_appr.admin

### Procedure

1. Navigate to **All** > **Approval Configurator** > **Approval Configurations**.
2. Click an approval configuration record in the list to set up the approval levels.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

3. Click **New** in the Approval Levels section.
4. On the form, fill in the fields.

**Approval Level form**

| Field | Description |
|---|---|
| Name | Name of the approval level. |
| Level | Stage of approval. |

**Note:** You cannot have more than one approval level for an approval configuration with the same level.

5. Click **Submit**.

## Set up approval rules

Set up rules for approvals at each approval level by selecting an approver type and the requirement of approval from either one or all the stakeholders. Define the filter conditions on the source table to which the approval rule is applied.

### Before you begin

Role required: sn_grc_appr.admin

### About this task

You can select specific approvers, approvers from the selected source table, dynamic approvers, or approvers that you choose to approve your business documents. For example, the approvers can be a risk administrator, a business impact analysis (BIA) owner, Business Continuity Management (BCM) admin, contributors, or one or all of them from the source table that you select.

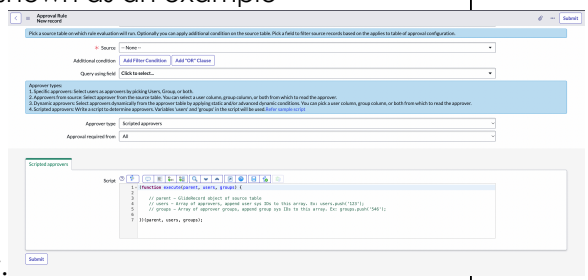
### Procedure

1. Navigate to **All** > **Approval Configurator** > **Approval Configurations**.
2. Click an approval configuration record in the list.
3. Click the approval levels record in the **Name** column of the Approval Levels section.
4. Click **New** in the Approval Rules section.
5. On the form, fill in the fields.

**Approval Rule form**

| Field | Description |
|---|---|
| Name | Name of the approval rule. |
| Source | Table to which the approval rule is applied. |
| Query using field | Field that connects the approving table and the source table. |
| Additional condition | Filter conditions applied on the source table. |
| Approver type | Type of approver. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | ◦ Specific approvers: Your choice of approvers.<br>◦ Approver from source: Users or groups from the source table.<br>◦ Dynamic approvers: Approvers selected dynamically from any table.<br>◦ Scripted approvers: Script to determine approvers. See the script shown as an example below.  <br>**Note:**<br>For security reasons, the Approver Configurator admin doesn't have write access to the **Script** field. The Approver Configurator developer has create and write access to the **Script** field on the Approval Rule form.<br>If you have the Approver Configurator admin role, you can set up an approval rule only with the following types of approvers from the Approver type list:<br>◦ Specific approvers<br>◦ Approver from source<br>For more information on the roles in the GRC: Approver Configurator application, see Roles installed with GRC: Approver Configurator. |
| Approval required from | One or more stakeholders from whom the approval is required. |
| Description | Brief note about the approval rule. |
| Approvers | |
| Approvers from | Approver table.<br>This field is available only if the Approver type is **Approver from source** or **Dynamic approvers**. Defaults to the source table if it's Approver from source. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Filter by | Conditions to filter records from the approver table.<br><br>This field is available only if the Approver type is **Dynamic approvers**. |
| Advanced | Option to set a scripted dynamic condition. |
| User field | User reference or list of approvers from the approver table. |
| Group field | User group reference as approver from the approver table. |
| Dynamic condition | Script field to apply advanced filter on approver table. |
| Users | One or more users designated as approvers. |
| Group | Group of approvers. |
| Scripted approvers | |
| Script | Script to determine approvers; **users** and **groups** in the script are selected as approvers. |

6. Click **Submit**.

## Roles installed with GRC: Approver Configurator

Various roles are installed with the activation of the GRC: Approver Configurator application.

**Roles installed with GRC: Approver Configurator**

| Role title [name] | Description | Contains roles |
|---|---|---|
| Approver Configurator admin<br><br>[sn_grc_appr.admin] | Create, read, update, and delete access to the Approval Configuration, Approval Levels, and Approval Rules tables.<br><br>**Note:** The Approver Configurator admin has read access to the **Script** field on the Approval Rule form. | None |
| Approver Configurator approver<br><br>[sn_grc_appr.approver] | Create, read, update, and delete access to the Approval tables. | None |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Roles installed with GRC: Approver Configurator (continued)**

| Role title [name] | Description | Contains roles |
|---|---|---|
| Approver Configurator developer<br><br>[sn_grc_appr.developer] | • Create, read, update, and delete access to the Approval Configuration, Approval Levels, and Approval Rules tables.<br>• Create and write access to the script field.<br><br>**Note:** The Approver Configurator developer has create and write access to the **Script** field on the Approval Rule form. | sn_grc_appr.admin |

## Confidential records

You can mark sensitive GRC records as confidential. You can then make sure that the right people have access to these records.

### Overview

You can mark sensitive GRC records as confidential by setting the confidential option for a record. By doing this action, you can ensure that only certain users or users from specific user groups can access these confidential records.

### Confidentiality property

A new option *`Enable record level confidentiality`* is available under GRC properties at the record level to enable confidentiality.

**Important:** The *`Enable record level confidentiality`* property is turned off by default. When it is enabled, it can't be turned off again.

The confidential records in GRC are listed under the GRC Confidential module. The GRC confidential records module is displayed in the application navigator only when you enable the *`Enable record level confidentiality`* property.

Starting with San Diego, the GRC Confidential Records module is available for the Audit Management, GRC core, Policy and Compliance Management, and Risk Management applications.

### Unmarking confidentiality on the record

When you unmark confidentiality on a record, allowed users and groups on that record will be removed and all the users will get access to the record based on ACL.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## User roles that are required to access the confidential records

Users with the GRC confidential user (sn_grc.confidential_user) role can access the confidential records. This role is for the users who are not GRC users but who want to access the GRC confidential records.

Users who have access and who are named in the record continue to have access to the record with the existing GRC role.

Consider the following examples for different roles:

- You are a risk user and you were given access to a risk record earlier. Now, you are part of the allowed users list for the same record. Therefore, even if you don't have the sn_grc.confidential_user role, you can access the record because you had access to this record earlier and your name is now listed on the allowed users list.
- Your name is listed on the record, but you don't have the sn_grc.confidential_user role. You must have the sn_grc.confidential_user role first to access the record.

When a record is marked as confidential, an email notification is sent out to the users and the user group members informing them about the assignment and the roles that are required to access the record. Every user that is listed in the Allowed users and Allowed groups list gets an email notification about the assignment of the record.

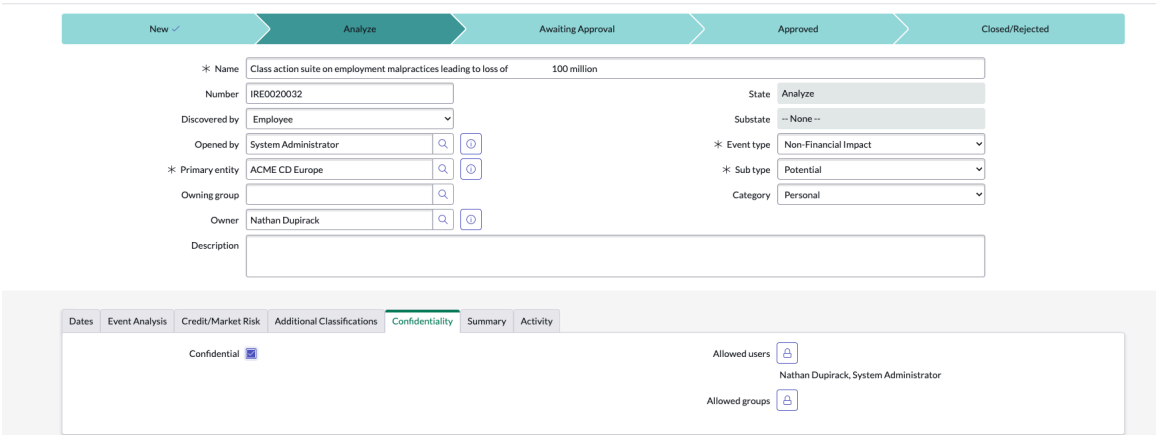
## Confidentiality tab on the form

The **Confidentiality** tab on the form displays the following lists and options:

- Confidential option: Enabling the **Confidential** option on the Confidentiality tab displays the Allowed users and Allowed groups lists as shown in the following figure.

  **Note:** A user with write access to the record can enable the **Confidential** option on the Confidentiality tab.

  **Confidentiality tab on a form**




- Allowed users list: When a record is marked as confidential, only the users in the Allowed users list have access to the record. A user who is listed in the Allowed users list should either have read access to the record or have the sn_grc.confidential_user role to access the confidential records.

  The logged-in user who enables the **Confidential** option gets auto-populated in the Allowed users list. The user who enables the **Confidential** option on the tab is auto-appended to the Allowed users list by default. Those users with write access to the record can unlock and update the Allowed users list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** There are no restrictions on which users can be added to the Allowed users list. A user who doesn't have the GRC role should have the sn_grc.confidential_user role to access the record. An email notification is also sent to the user about the role requirement.

- Allowed groups list: When a record is marked as confidential, only the users that are listed in the Allowed groups list have access to the record. Those users with write access to the record can unlock and update the Allowed groups list.

  **Note:** Confidential records are visible to the users who are listed in the Allowed users or Allowed groups list. By default, the administrators can also view the confidential records. If you do not want the administrators to view the confidential records, follow the steps mentioned in KB1497382.

Users who don't have the GRC user role but are listed in the Allowed users list or Allowed groups list can be assigned with the sn_grc.confidential_user role to access the confidential records.

Confidentiality is supported on the following tables.

**Tables on which confidentiality is supported**

| Table label | Table name | Application scope | Users that get auto-populated in the allowed users list | Groups that get auto-populated in the allowed groups list |
|---|---|---|---|---|
| Audit task | sn_audit_task | GRC: Audit Management | Assigned To, Engineering lead, Engineering auditors, Engineering approvers | Not applicable |
| Engagement | sn_audit_engagement | GRC: Audit Management | Auditors, Approvers, Engagement lead | Not applicable |
| Evidence request task | sn_grc_advanced_erc_evidence_respo | GRC: Advanced Core | Requester, Assigned To, Approvers, Watchlist, Requested on behalf of | Assignment Group |
| Issue | sn_grc_issue | GRC: Profiles | Assigned to, Issue Manager, Opened by | Issue Manager Group,Assignment Group |
| Observation | sn_audit_advanced_observation | GRC: Advanced audit | Owner, Respondent, Peer Reviewer, Reviewer, Watch list Users, Engagement | Assignment Group |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tables on which confidentiality is supported (continued)**

| Table label | Table name | Application scope | Users that get auto-populated in the allowed users list | Groups that get auto-populated in the allowed groups list |
|---|---|---|---|---|
| | | | lead, Engineering auditor, Engineering approver | |
| Policy exception | sn_compliance_policy_exception | GRC: Policy and Compliance Management | Requester, Approver, Watch list | Approval Group |
| Remediation task | sn_grc_task | GRC: Profiles | Assigned to, Watch list, Issue Manager, Issue Assigned To | Not applicable |
| Risk events | sn_risk_advanced_event | Advanced Risk | Current logged in user, Owner, Approver | Owning group, Approval groups |
| Disclosure | sn_esg_disclosure | ESG Management and Reporting | Logged in user, reviewer, assigned to | Not applicable |
| Material topic | sn_esg_material_topic | ESG Management and Reporting | Logged in user, reviewer | Not applicable |
| Metrics | sn_grc_metric | ESG Management and Reporting | Logged in user, enterprise owner, data owner | Enterprise owner group, data owner group |
| Metric definitions | sn_grc_metric_definition | ESG Management and Reporting | Logged in user, enterprise owner, data owner | Enterprise owner group, data owner group |
| Composite metric definitions | sn_grc_composite_metric_definition | ESG Management and Reporting | Logged in user, enterprise owner | Enterprise owner group |

Starting with Utah, confidential configuration for all the Out Of the Box confidentiality enabled GRC tables except sn_esg_material_topic, sn_grc_metric, sn_grc_metric_definition, sn_grc_composite_metric_definition, are shipped to sn_grc_confidentiality_configuration table. You can update and remove the user and group fields that are auto-populated into allowed users and groups of a record from this configuration.

To know more about the confidentiality feature, see KB1218856.

### Configure confidentiality in your GRC tables

To enable confidentiality in your GRC tables, you must perform additional configuration, such as updating the client scripts and updating access control lists (ACLs). After you update the

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

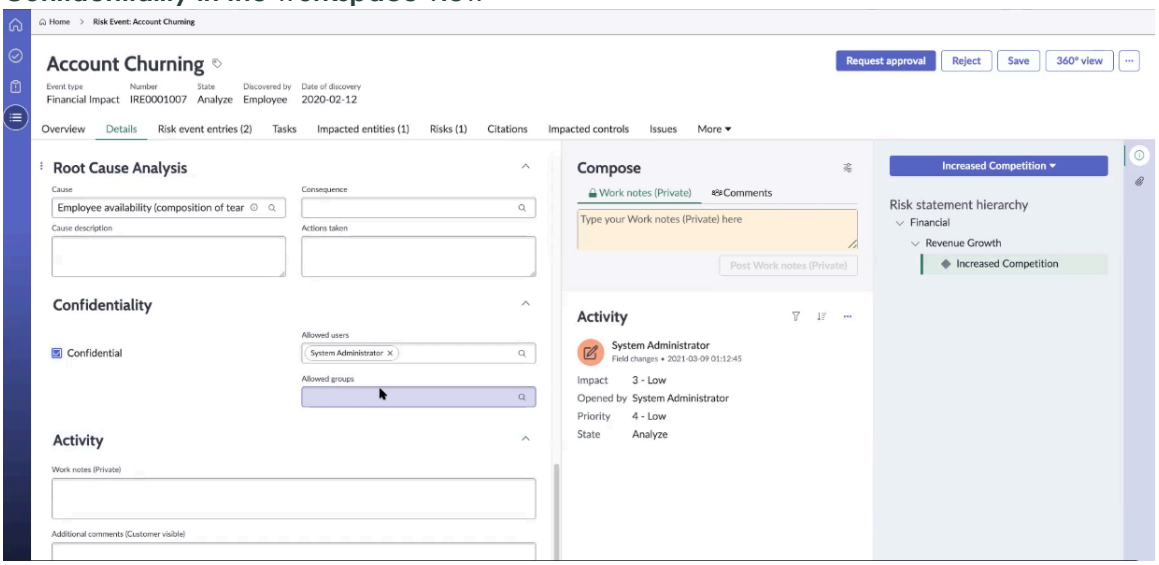
configuration for a specific ServiceNow platform table, the confidentiality functionality can be used on those table's forms.

For information on how to enable confidentiality in your GRC tables, see KB1497382.

**Note:** You must log in to Now Support to view the Knowledge Base articles.

You can also enable Confidentiality on a form in the workspace view as shown in the following figure.

**Confidentiality in the workspace view**




## Create a confidential record

Create a record and mark it as confidential so that you can make sure that only the users with a specific role can access it.

### Before you begin

Role required: sn_grc.admin, sn_grc.business_user who has opened the risk event, sn_audit.user, sn_compliance.user, sn_esg.user, sn_risk.user

### Procedure

1. Navigate to **All > Administration > GRC Properties**.
2. Select **Yes** for **Enable record level confidentiality** property and click **Save**.
   Perform the following steps by logging in with the sn_grc.business_user role or a module specific role as defined in the Role required section.
3. Navigate to the record that should be marked as confidential and click **Confidentiality** tab.
4. On the **Confidentiality** tab, select the **Confidential** option.
   The Allowed users and Allowed groups lists are displayed. The user who enables the **Confidential** option is auto-appended to the Allowed users list by default.
5. To add more users, update the Allowed users list.
6. To add more groups, update the Allowed groups list.
7. Click **Update**.

### Result

The selected record is marked as confidential. Only the users who belong to the Allowed users list or the Allowed groups list can access this confidential record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Configure confidentiality in GRC tables

You can create a confidentiality configuration record in your GRC tables.

### Before you begin

Before you begin the confidentiality configuration on your table, you must create three new columns in the table that you want to enable confidentiality in.

Role required: sn_grc.admin.

#### Fields to enable confidentiality

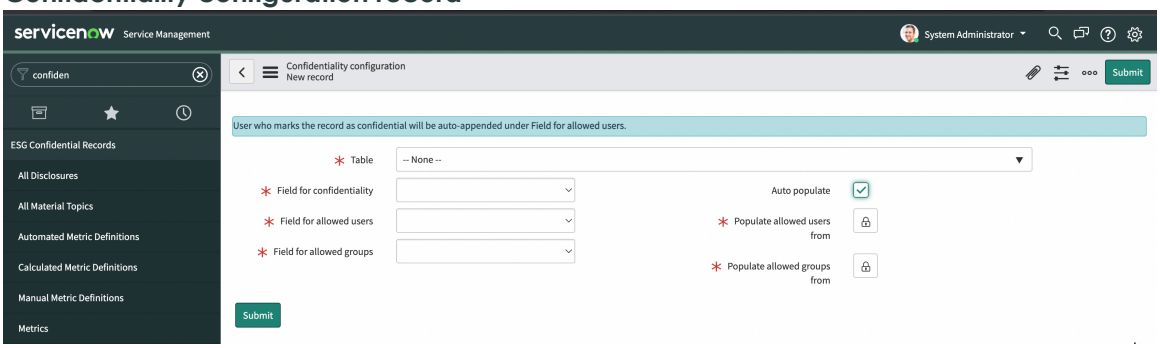
| Type | Comments | Example column name | Description |
|---|---|---|---|
| Boolean | Confidential | u_confidential | Flag that marks or unmarks whether a field is confidential. |
| List, Reference to sys_user table | Allowed users | u_allowed_users | Field that contains the list of users who can access the confidential record. |
| List, Reference to sys_user_group table | Allowed groups | u_allowed_groups | Field that contains the list of user groups who can access the confidential record. |

For more information, see KB1497382.

### Procedure

1. Navigate to **All** > **GRC Administration** > **Confidentiality Configuration** and click **New**.
2. In the new confidential configuration form, fill in the fields that are required for enabling confidentiality for the GRC tables.
   For more information about the fields, see Confidentiality configuration form.

#### Confidentiality configuration record




3. Click **Submit**.

### Result

Confidentiality is enabled for the GRC table that you selected.

#### Confidentiality configuration form

The Confidentiality configuration form is used for the configuration of the confidential records for your GRC tables.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Confidentiality configuration form**

| Field | Description |
|---|---|
| Table | Table that you want to add the Confidentiality feature in. |
| Field for confidentiality | Boolean field where you can enable for confidentiality in. |
| Field for Allowed users | Field where you can add the allowed users who can access the confidential records. |
| Field for Allowed groups | Field where you can add the user groups that are allowed to access the confidential records. |
| Populate allowed users from | Field where the allowed users are automatically filled in based on the list of columns in the GRC tables. |
| Populate allowed groups from | Field where the allowed user groups are automatically filled in based on the list of columns in the GRC tables. |

**Note:** **Populate allowed users from** and **Populate allowed groups from** fields appear only when the **Auto-populate** field is selected.

## Configuring confidential inheritance in your tables

You can set up confidentiality inheritance in the tables that are already configured in the confidentiality configuration module. In the GRC application, whenever a parent record is marked or unmarked as confidential, its related table records are also marked or unmarked as confidential.

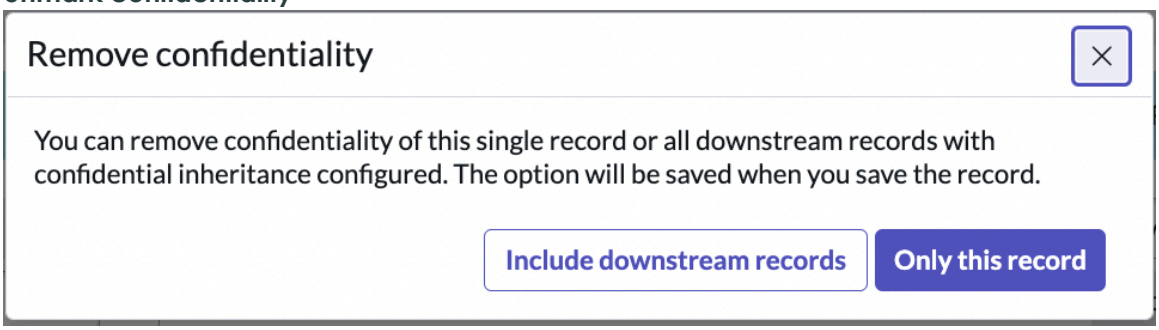
## Overview

When you mark an issue as confidential, a related remediation task is automatically marked as confidential. For example, let's look at issue A. Issue A has the remediation tasks P, Q, and R. If issue A is marked as confidential, the remediation tasks P, Q, and R are also marked as confidential. The allowed users and groups are automatically appended based on the remediation task's confidentiality configuration record. Issue A's allowed users and groups are automatically appended to the inherited records P, Q, and R.

When an issue's confidentiality is unmarked, the corresponding confidentiality of a remediation task is also unmarked. Let's look at issue A again. Remember that issue A has the remediation tasks P, Q, and R. If the confidentiality is unmarked for issue A, then a dialog box appears with a question about whether it's okay to unmark the confidentiality for all the related tasks P, Q, and R or only for issue A. Based on what the selection is in the following example, the related records are unmarked as confidential.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Unmark confidentiality**




As shown in the example dialog box, if **Include downstream records** was selected, then the confidentiality is unmarked for all the downstream records. If **Only this record** was selected, the confidentiality is unmarked for that single record only.

If you have access to the related confidential records and remove the confidentiality for a parent record, then the related records are also non-confidential.

**Note:** An inheritance configuration should exist between the parent and inherited tables.

## Examples of confidentiality inheritance

Inheritance works only at the point of marking a parent record as confidential. Let's look at the following two examples:

1. When a parent record is marked as confidential, the related non-confidential records are also marked as confidential due to the inherited configuration. But, if a related record is added later, it isn't automatically marked as confidential.
2. Whenever confidentiality is marked on a parent record and the inheritance isn't passed to the related records, the changes that are made later to the allowed users and groups of the parent record are not inherited in the related records.

For more information about the confidentiality inheritance configuration, see KB1213404
You must log in to the Now Support to view the Knowledge Base articles.

### Create confidentiality inheritance

Create confidentiality inheritance in the tables that are already configured in the confidentiality configuration module. In the GRC application, whenever a parent record is marked or unmarked as confidential, its related table records are also marked or unmarked as confidential.

**Before you begin**
Before you begin confidentiality configuration on your table, you must create three new columns in the table that you want to enable confidentiality in.

Role required: sn_grc.admin.

**Fields to enable confidentiality**

| Type | Comments | Example column name | Description |
|---|---|---|---|
| Boolean | Confidential | u_confidential | Flag that marks or unmarks whether a field is confidential. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Fields to enable confidentiality (continued)**

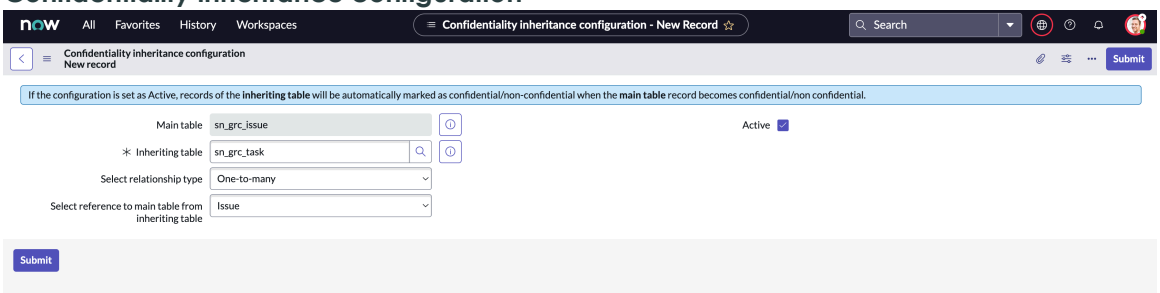
| Type | Comments | Example column name | Description |
|---|---|---|---|
| List, Reference to sys_user table | Allowed users | u_allowed_users | Field that contains the list of users who can access the confidential record. |
| List, Reference to sys_user_group table | Allowed groups | u_allowed_groups | Field that contains the list of user groups who can access the confidential record. |

For more information, see KB1096093.

## Procedure

1. Navigate to **All** > **GRC Administration** > **Confidentiality Configuration**.
2. Select the table that you want to configure the inheritance in.
3. In the Confidentiality inheritance configurations related list, select **New**.
4. On the form, fill in the fields.
   The following example shows how to configure the confidentiality inheritance. For more information about the fields, see Confidentiality Inheritance Configuration form.

**Confidentiality inheritance configuration**




5. Select **Submit**.

> **Note:**
>
> This configuration doesn't affect the existing confidentiality of the records in the parent and inheriting tables.
>
> Only records that are marked as **Active** support the inheritance.

## Result

A new inheritance configuration record is created under the confidentiality inheritance configuration related list.

### Confidentiality Inheritance Configuration form

Use the Confidentiality Inheritance Configuration form in the GRC application to create the inheritance configuration record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Confidentiality Inheritance Configuration form**

| Field | Description |
|---|---|
| Active | Option that when selected marks the inheriting tables of the main table as confidential. |
| Main table | Main table that shows the table that is selected in the confidentiality configurations. |
| Inheriting table | Table that has records where the confidentiality is marked or unmarked. |
| Select relation type | Relation types that exist between the main and inheriting table. |
| Select relationship table | Option to select a relationship table. The **Select relationship table** field appears only when you select the relation type as **Many to Many** or **Scripted relationship**. |
| Select reference to main table from relationship/inheriting table | Reference to the main table and inherited tables. |

**Note:** If only one relationship exists between the main table and the inheriting table fields of the form, the remaining fields are automatically filled in and hidden on the form.

## User hierarchy

With a user hierarchy, your managers can see the records of those users who report to them.

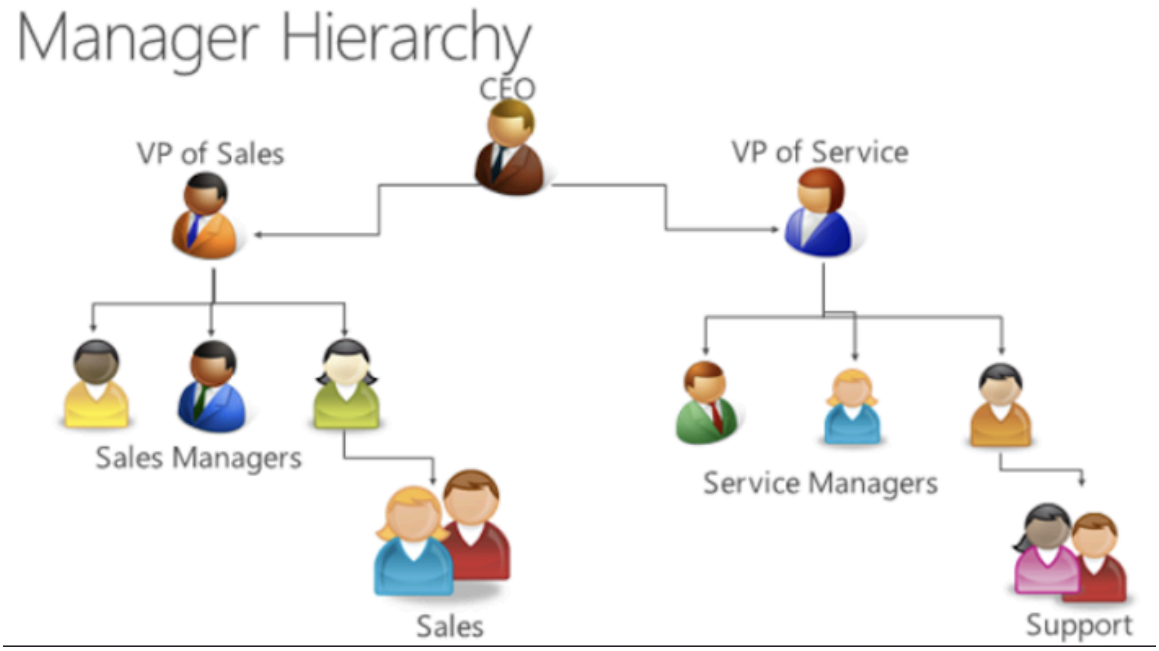
The user hierarchy is based on the configuration in the sys_user table. The user hierarchy is stored separately for the GRC tables.

To understand how a user hierarchy works, let's look at the following example. Users Abel and Jack report to Adam. Adam reports to Daniel. With a user hierarchy, Adam can view the work performed by Abel and Jack. Similarly, Daniel can view the work performed by Adam, Abel, and Jack.

Let's see another example of a manager and a user hierarchy.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Manager and user hierarchy**




In this example, the sales manager can see the data that the sales team has submitted. The VP of sales can see the data or reports that are submitted by the sales managers and the sales team.

The VP of service can see the data that is submitted by the service managers and the support team. The CEO of the organization can see the work performed by both sales and service teams.

## Enabling the properties for the user hierarchy functionality

As a GRC administrator, you can enable the following properties under the GRC properties module in an instance.

**User hierarchy properties**

| Property | Action |
|---|---|
| *Enable user hierarchy access control* | Enable the user hierarchy functionality by selecting the **Yes** option on the *Enable user hierarchy access control* property. This property is turned off by default. After you enable this property, you can also turn it off again. |
| *Frequency of user hierarchy recalculation* | Use the *Frequency of user hierarchy recalculation* property to calculate the user hierarchy for all the records in the sn_grc_user_hierarchy_configuration table. The property is set to **Weekly** by default.<br><br>To calculate the user hierarchy for the records at different intervals, select *sn_grc.user_hierarchy_sync_frequency* |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**User hierarchy properties (continued)**

| Property | Action |
|---|---|
| | and change the schedule from **Weekly** to **Daily** or **Monthly**. |
| *Maximum batch size while recalculating hierarchy for user hierarchy records* | Use the *Maximum batch size while recalculating hierarchy for user hierarchy records* property to process the records in a maximum batch size so that you can recalculate the user hierarchy of the records. This property is set to 1000 by default.<br><br>To recalculate the user hierarchy of the records, select the property and update the maximum batch size to an integer value. |

**Note:** After you enable the user hierarchy properties, the user hierarchy functionality is supported only in certain sets of tables. You can learn more about these tables in the next section.

## Tables that are used to support the user hierarchy functionality

The following tables are used to support the user hierarchy functionality.

**Tables that are used to support the user hierarchy functionality**

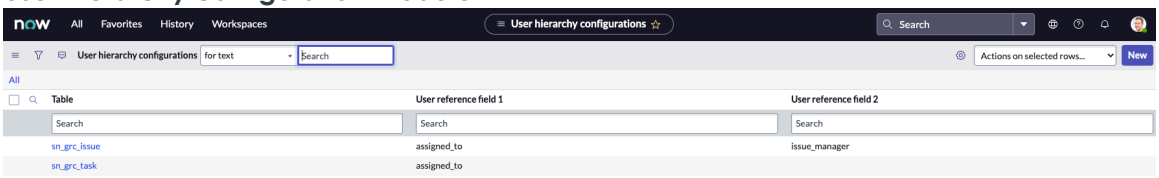
| Table | Description |
|---|---|
| sn_grc_user_hierarchy | Table that displays the name of the user, the managerial hierarchy, and the last synchronized details. As a user with the sn_grc.user_hierarchy_reader role, you can read the records in this table. No other user can manually create, update, or delete the records in this table. |
| sn_grc_user_hierarchy_configuration | Table that contains a separate record for each table where the user hierarchy access control is enabled. As a GRC administrator, you can manually create and delete the records in this table. As a user with the sn_grc.user_hierarchy_admin role, you can also read or update the records in this table. |

## User hierarchy configurations module

The User hierarchy configuration module is displayed in your instance only after you enable the user hierarchy properties. The User hierarchy configuration module, which is shown in the following example, lists the tables on which you have enabled the user hierarchy functionality.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### User hierarchy configuration module




Access control lists (ACLs): By default, a few access control lists are shipped with the GRC application, and they are stored in the sys_security_acl table. You can define a filter condition to check if the user hierarchy access control is enabled. You can create your own access control lists depending on your configuration and requirements.

For information on how to configure the user hierarchy access control on your custom tables, see KB1095957 .

**Note:** You must log in to Now Support to view the Knowledge Base articles.

## Create a user hierarchy configuration record

Create a user hierarchy configuration record for a table so that you can enable your managers to view the records of the users who report to them.

### Before you begin

Role required: sn_grc.admin

### Procedure

1. Navigate to **All** > **GRC User Hierarchy > User hierarchy configuration**.
   The tables where you have enabled the user hierarchy access control are displayed.
2. Click **New**.
3. On the form, fill in the fields.

#### User hierarchy configuration form

| Field | Description |
|---|---|
| Table | Table that you can use to configure the user hierarchy. For example, Issue [sn_grc_issue]. |
| Active | Option to enable the user hierarchy. When you enable this option, the user hierarchy functionality is enabled on the table records. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| User reference field 1 | Field that corresponds to User reference field 1 in the user table. For example, you can select the value of the User reference field 1 as Assignee or Assigned to. |
| User reference field 2 | Field that corresponds to User reference field 1 in the user table. For example, you can select the value of the User reference field 2 as Approver or Issue manager. |
| User hierarchy field 1 | Field to configure the user hierarchy for User reference field 1. |
| User hierarchy field 2 | Field to configure the user hierarchy for User reference field 2. |
| User hierarchy status field | Field that represents the status of the user hierarchy processing for the selected table. |
| Triggered event | Event that is used to recalculate the user hierarchy in the source table records. |

For configuring the user hierarchy on your table, see KB1095957.

4. Click **Submit**.

## User group-based access on the GRC tables

You can allow a set of users to access only specific records by creating user groups on the GRC tables. When you have created the user groups, you can segregate your data based on a specific criteria and allow only those users who belong to a user group to view the data.

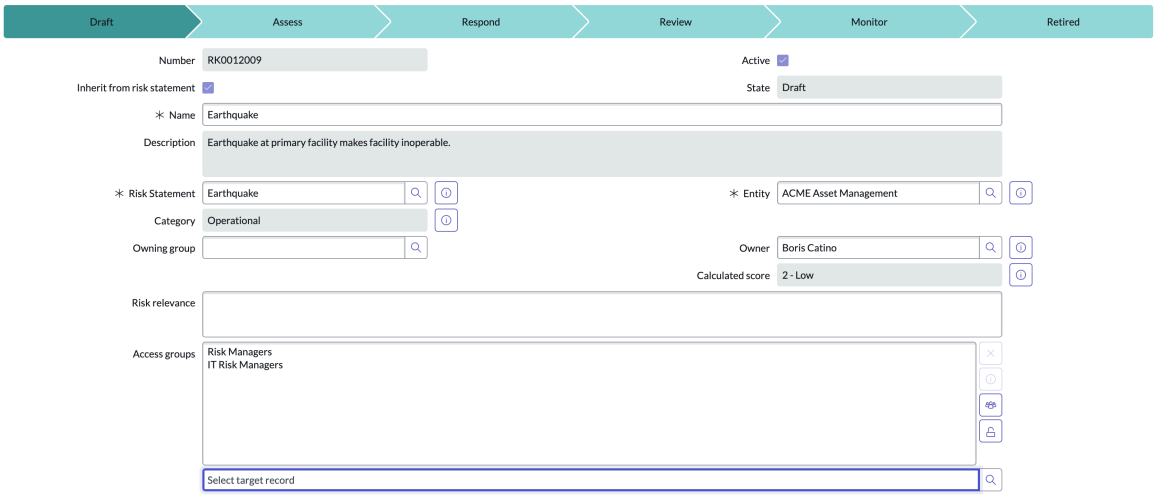
**Note:** User group-based access is not enabled on any ServiceNow tables as part of the base system. To implement the feature and to configure the Access groups option on any GRC form, follow the steps listed in the KB1514113.

To view the Access groups option on the respective tables where you have configured user group-based access, you must enable the *Enable access groups* property in the GRC Properties module.

The following example shows the Access groups option in the form that appears when you enable user group-based access. The layout of the form depends on your configuration.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Access groups option in the form




When a value is selected for the Access groups list, only the members of the groups that are mentioned in the list can access the data within the same role.

Consider the following example. Within the Risk Managers access group, you have two managers who can work on a financial risk and other managers who can work on an operational risk. By giving the same risk manager role to all the managers in this access group, the first two managers can be assigned to the financial group and the other managers can be assigned to the operational risk group.

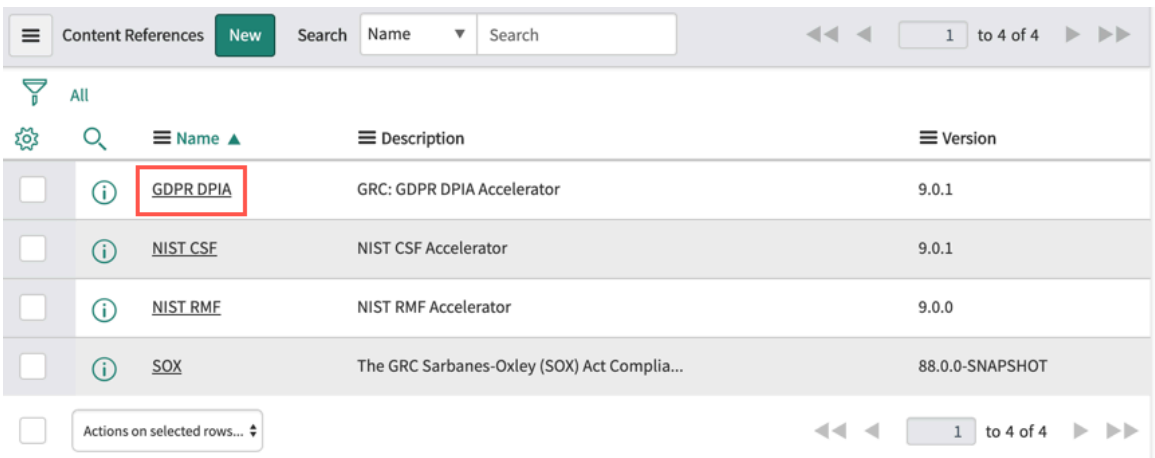
## Content references in GRC

You can add tags to virtually any type of record defined in GRC applications that reference GRC content packs, integrations, use case accelerators, or any new regulations that use those records. After the records have been tagged, you can filter the content reference tags to identify which records are used within each application.

For example, you can tag all SOX control objectives that are scoped for the NIST RMF integration. You can also create reports that show relevant records that are tagged for specific integrations, use case accelerators, and so forth.

After records have been tagged, you can access all of the content references used within a specific GRC application by viewing the Content References module under each. In Policy and Compliance, for example, you can view all tagged records for the GDPR DPIA use case accelerator in a series of related lists.

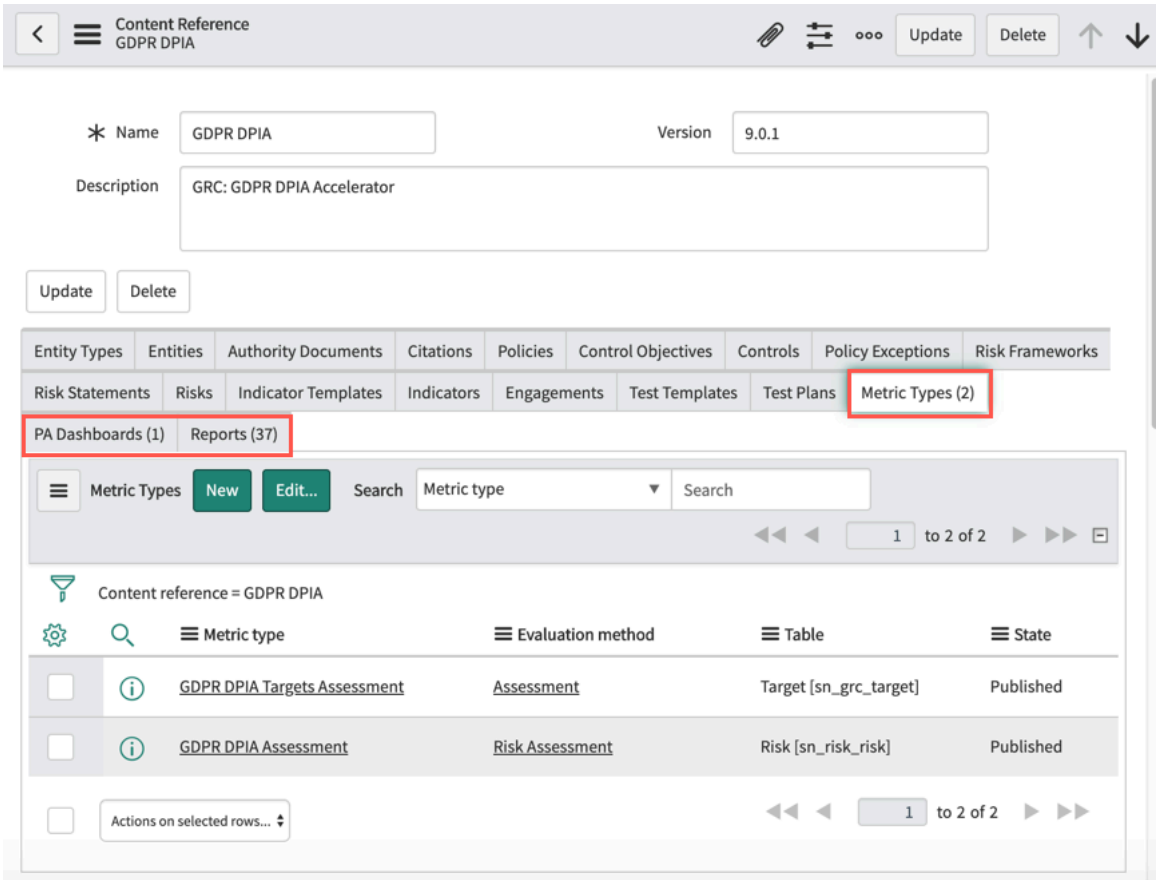
### Content reference list




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After selecting GDPR DPIA, a series of related lists show all records tagged with content references to the GDPR DPIA Use Case Accelerator.

**Content references for GDPR DPIA**




## Records you can tag with content references

In the GRC Audit Management, Policy and Compliance Management, and Risk Management applications, you can tag any of the following types of records.

**Note:** Not all of these records are available within each of the GRC applications listed above The related lists displayed in each of the applications, however, include all of the record types regardless of whether they are available.

- Authority Documents
- Citations
- Control Objectives
- Controls
- Engagements
- Entity Types
- Entities
- Indicator Templates
- Indicators
- Metric Types
- Dashboards

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Policies
- Policy Exceptions
- Reports
- Risk Frameworks
- Risk Statements
- Risks
- Test Plans
- Test Templates

## Add content reference tags to records

As you are analyzing any of the many types of records available in GRC applications, it is easy to add a content reference tag so the record can be included when you perform searches for records associated with a given integration, content pack, use case accelerator, and so forth.

### Before you begin

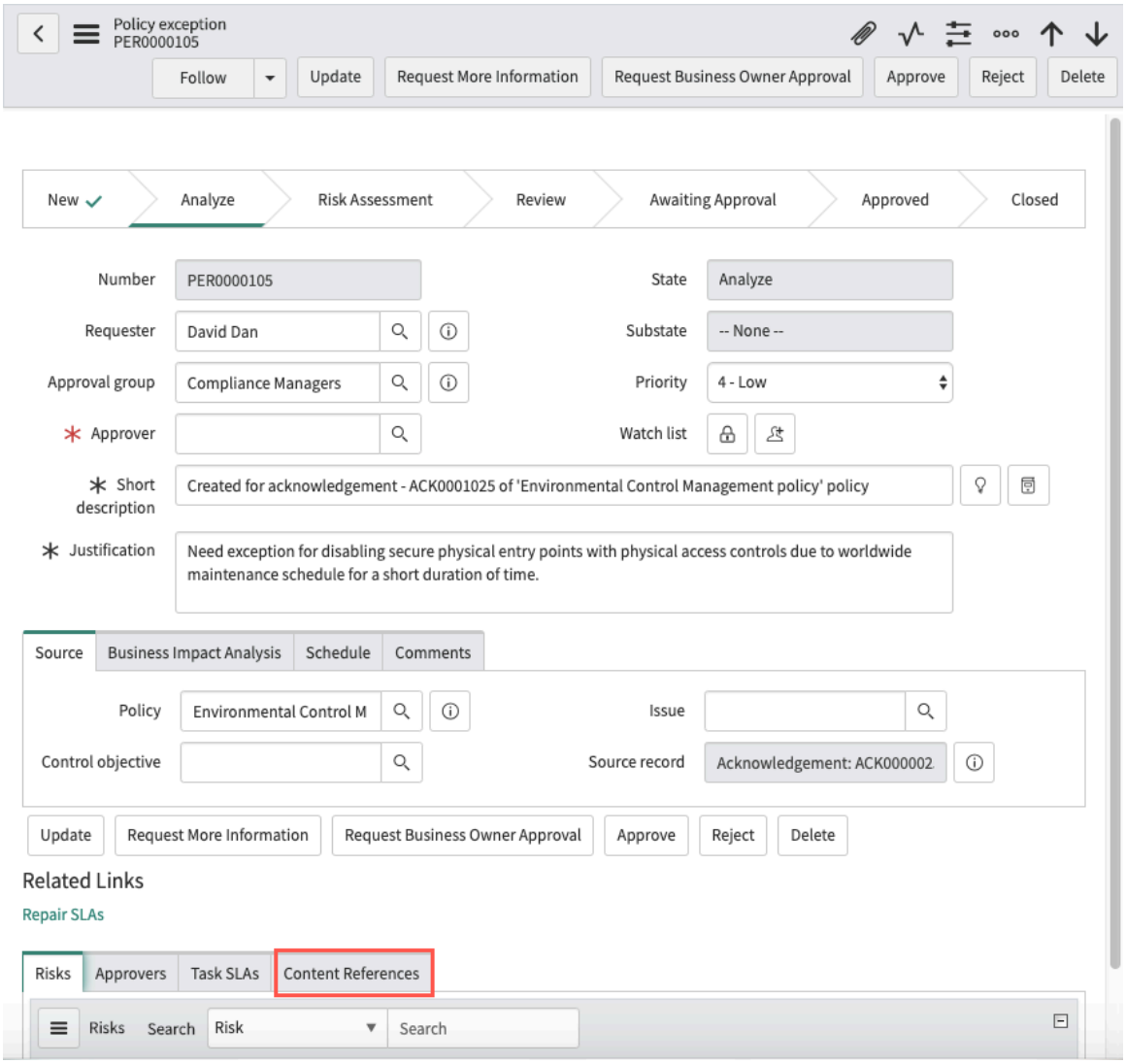
Role required: admin

### Procedure

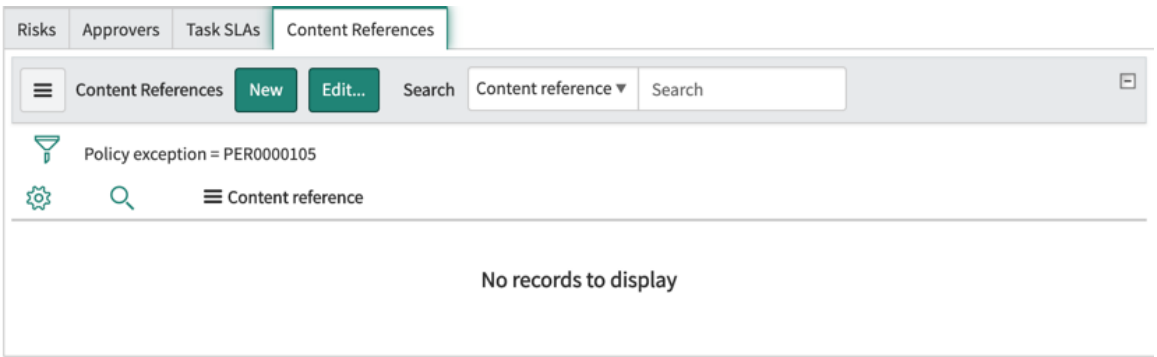
1. Navigate to **Policy and Compliance** > **Policy Exceptions** > **My Policy Exceptions**, and open a specific policy exception record.
   If you are already working within a specific GRC application, open the record to which you want to add a content reference tag. Otherwise, navigate to the record.

   **Note:** For the sake of example, a Policy Exception record is used to illustrate how to add a content reference to a GRC record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

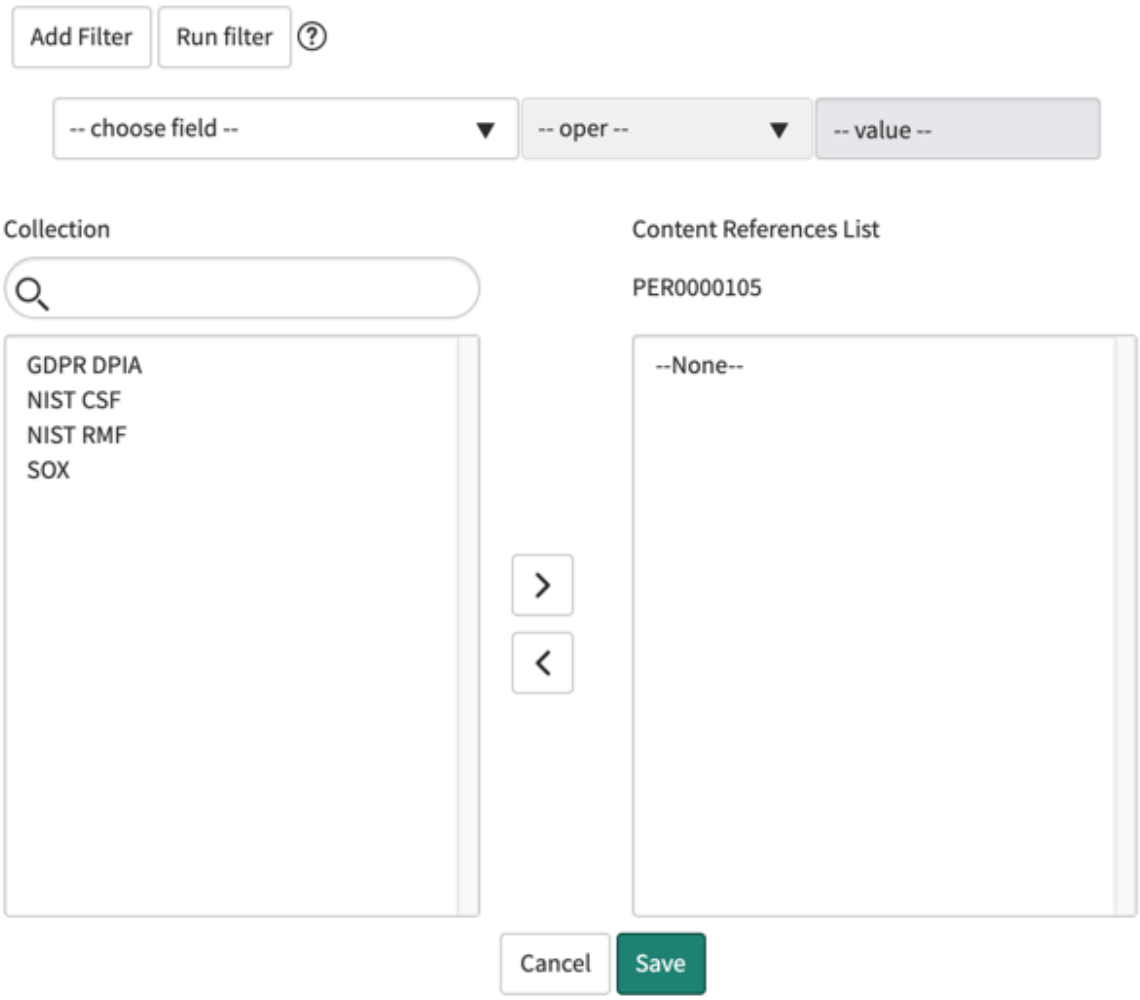



**2.** Scroll down and click the **Content References** related list.

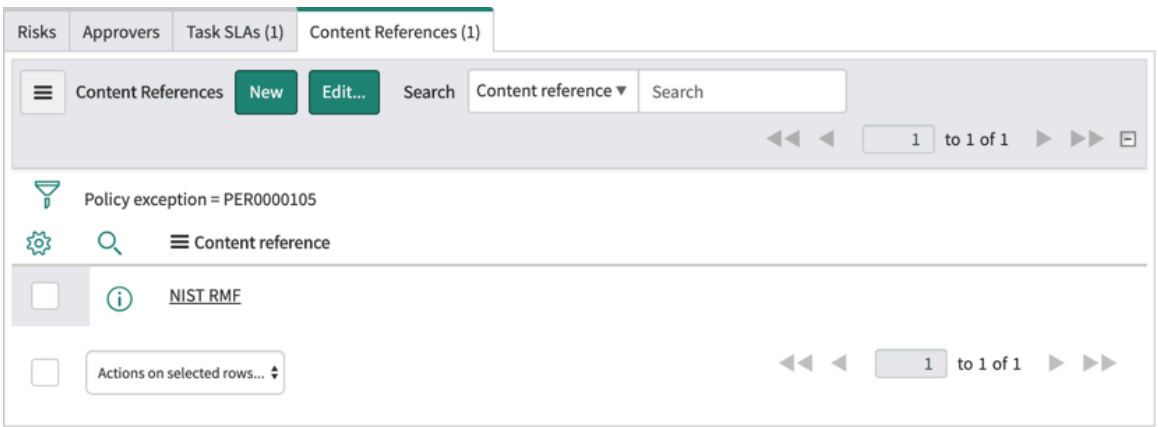



**3.** Click **Edit**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.



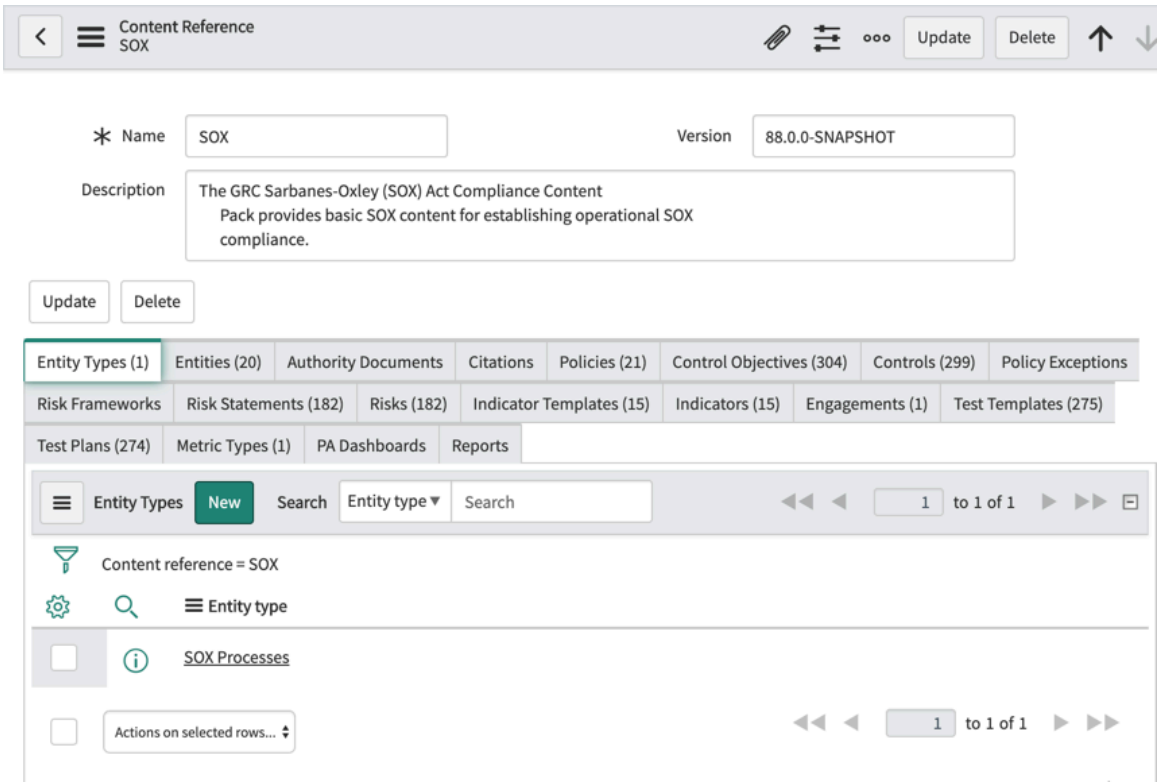

4. Click **Save**.
   Move the integrations, use case accelerators, and so forth to which you want to associate with this policy exception record from the **Collection** box to the **Content References List**, then click **Save**. In this example, policy exception record PER0000105 has been tagged as being associated with the NIST RMF Use Case Accelerator.




5. Navigate to the **Content References** module under that application and select the associated use case accelerator.
   To view all records tagged for a specific use case accelerator within a specific GRC application, For example, to see all records tagged with content references in Risk

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Management for the SOX content pack, navigate to **Risk** > **Administration** > **Content References**, and click **SOX**.




6. Click any of the related lists that show a number to see the records tagged as content references for SOX.

## Create content reference tags

You can define new content reference tags, as needed, to accommodate new regulations as they arise. You can define new tags in any GRC application, and they are then available in all GRC applications.

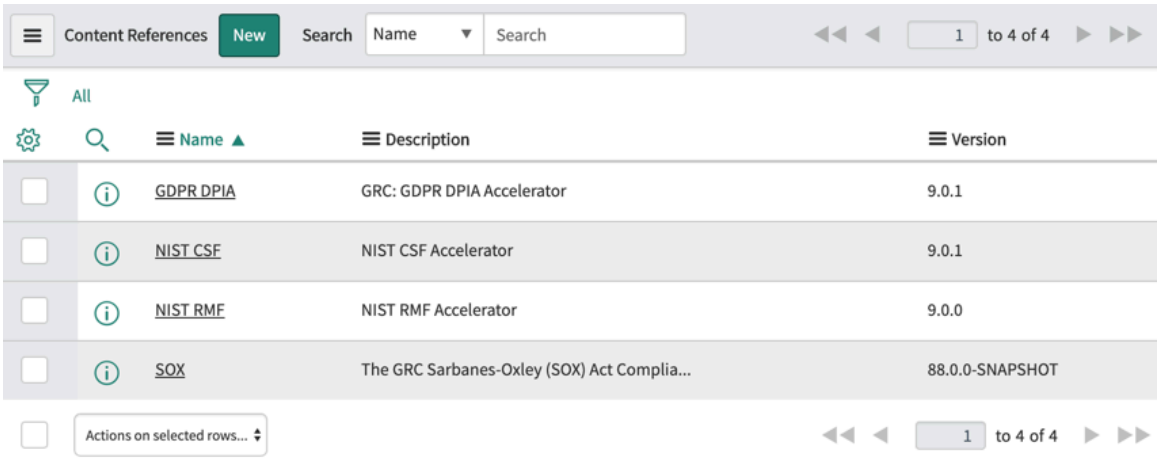
### Before you begin

Role required: admin

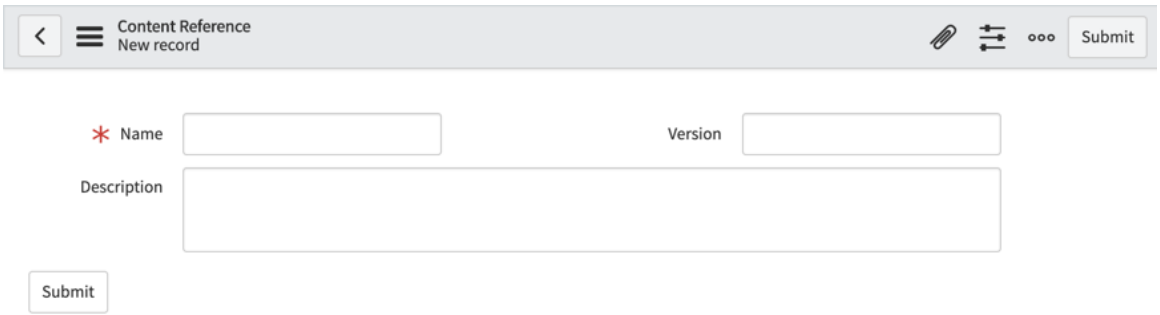
### Procedure

1. Navigate to the Content References module in any GRC application.
   For example, you can navigate to **All** > **Audit** > **Administration** > **Content References**

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.




2. Click **New**.




3. Provide a **Name**, **Version** number, and **Description** for the new tag.

   **Note:** The **Version** number can be the software version released from the ServiceNow Store

4. Click **Submit**.
   The new content reference tag is added to the list and is available from the Content Reference module in the GRC Audit Management, Policy and Compliance Management, and Risk Management applications.

## Manage issues

You can measure the effectiveness of your company's risk management program by how quickly and completely it identifies and reacts to risk and compliance issues.

Issues can be submitted using two methods, depending on the type of user involved:

- Employees and business users within your company can self-identify an issue and submit it via the ServiceNow® Service Portal. Following submission, a triage issue is automatically created and the issue triage process begins.
- GRC users can manually create an issue from within their instance to document audit observations and remediations, and compliance and risk issues.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** Various types of issues can also be automatically generated under the following conditions (these types of issues are not triaged):

- Control issue: Created when a control attestation is completed, indicating that the control is not implemented, or when an indicator fails.
- Control test issue: Created when a control test is closed complete with the control effectiveness set to **Ineffective**.

## The goals of issue management

The goals of issue management include:

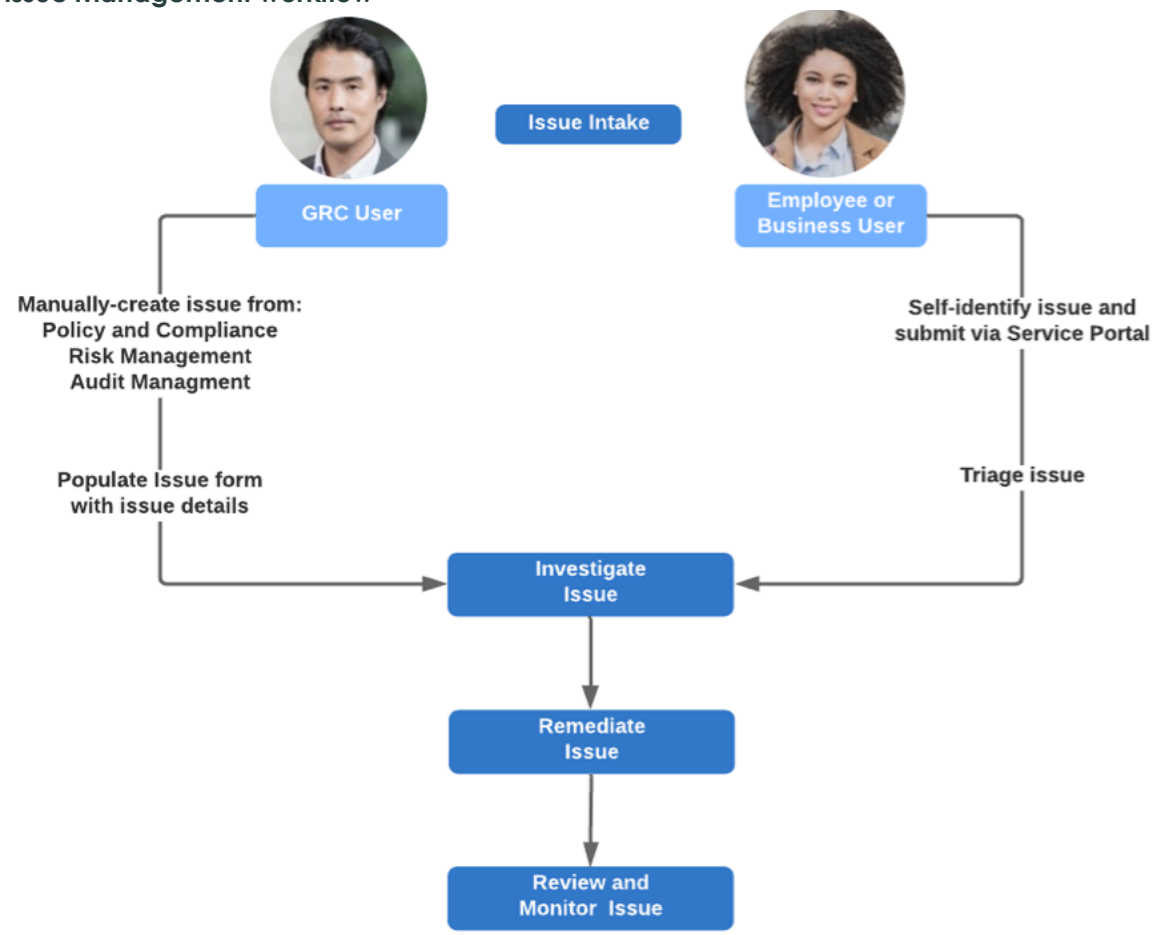
- Eliminating noise.
- Consolidating duplicate issues.
- Focusing on issues that expose the organization to the greatest risk.
- Identifying and prioritizing remediation actions.
- Identifying new issues across the business operations.
- Analyzing operational weakness in policies, processes, and controls.

## Issue management workflow and life cycle

By remediating issues, controls can be kept compliant, and risk can be mitigated. The Issue Management workflow and life cycle are illustrated and described here.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Issue Management workflow




### Issue Management life cycle

| Stage | Description |
|---|---|
| Issue intake | As described earlier, issues can be submitted using two methods, depending on the type of user involved:<br>• Employees and business users within your company can self-identify an issue and submit it via the ServiceNow® Service Portal. Following submission, a triage issue is automatically created and the issue triage process begins.<br>• GRC users can manually create an issue from within their instance. These types of issues are not triaged. |
| Investigate the issue | During the investigation phase, it is determined whether the issue requires additional study. If a triage is being performed, the triage issue is assigned to a triage team for analysis. The triage team may request more information from the issue creator. The team can also optionally send the issue to the compliance manager, risk |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Issue Management life cycle (continued)**

| Stage | Description |
| --- | --- |
| | manager, or triage manager with a triage result. |
| Remediate the issue | After the team has confirmed the issue, the necessary steps to remediate it are performed. If a triage was performed, the triage issue is converted into an actual issue or risk event. The team may also decide to track the issue as a recommendation or close it as a non-issue. |
| Review and monitor the issue | Prior to closing the issue, the policy owner reviews and approves it. The review also allows the organization to:<br>• track past due tasks<br>• benchmark issue timelines<br>• identify where losses could have been mitigated<br>• reduce gaps in the future |

## Tracking your issues in the Workspace

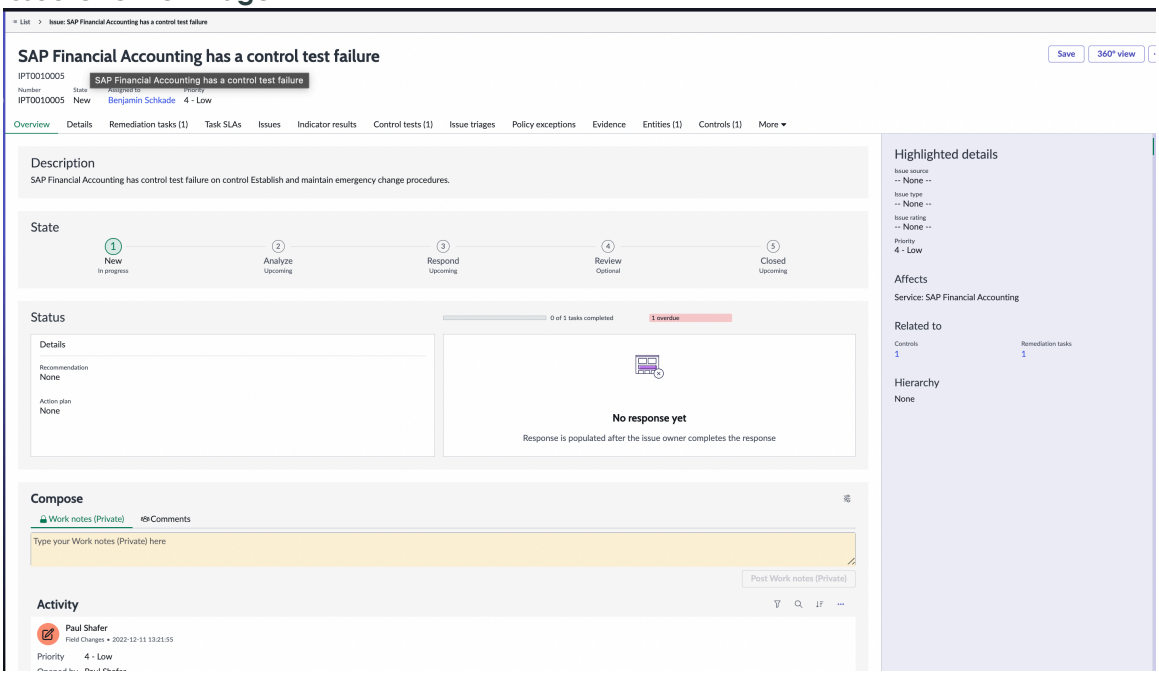
You can track all your issues or one specific issue by looking at the Issue form in the Workspace. Issues are listed under the **Issues** module in the list view of the Workspace.

## Overview

The issue form displays the details about your issues. You can see information about an issue's description, state, status, work notes, and what activity has occurred so far. The information about an issue is organized in different tabs such as the **Overview** tab and the **Details** tab as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Issue Overview Page




In the **Details** tab, you can find information about the issue, assignment, schedule, issue grouping, action plan, confidentiality, and activity and settings.

**Note:** The details section has been removed from the **Details** tab.

## Associating objects that are related to an issue

You can associate objects, such as the control, risk, risk event, entities, engagements, control objectives, risk statements, policies, authority documents, or processing activities, or remove the existing objects that are related to the issue.

For example, consider an entity that you can select as a related list. You can either add the other related entities or remove the existing entities by using the **Add** or **Remove** UI buttons of the entity form.

The related lists on the issue form display the dependencies that are related to the issues. The following table lists a description of the tabs and sidebar on the Issue form.

### Tabs and sidebar on the Issue form

| Tab | Description |
|---|---|
| Overview | Overview of an issue, such as the description, state, status, work notes, and activity. |
| Details | Details about an issue, such as the assignment, schedule, issue grouping, action plan, confidentiality, activity, settings, and work notes. |
| Highlighted details | Highlighted information, such as the issue source, issue type, issue rating, priority, effects, related to, and hierarchy. |
| Affects | Entities that are affected by this issue. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Tabs and sidebar on the Issue form (continued)**

| Tab | Description |
|---|---|
| Related to | Count of the different objects that are affected by this issue such as the controls, risks, policies, authority documents, engagements, regulatory change tasks, remediation tasks, and risk events. |
| Hierarchy | Issue hierarchy. |

The following table lists the related lists in the Issues section.

**Related lists in the Issues section**

| Related lists | Description |
|---|---|
| Remediation tasks | Details of the remediation tasks, such as the name, number, state, assigned to, priority, planned end date, and actual date. |
| Task SLAs | Details of the task service level agreements (SLAs), such as the SLA definition, type, target, stage, business time left, business-elapsed time, business elapsed percentage, start time, and stop time. |
| Issues | Details of the related issues, such as the name, number, issue source, issue type, state, issue manager, assigned to, priority, and due date. |
| Indicator results | Details of the indicator results, such as the name, result, indicator, and data owner. |
| Control tests | Details of the control tests, such as the name, number, parent, assigned to, state, planned start date, and planned end date. |
| Issue triages | Issue triages details, such as the name, number, source, issue type, state, substate, triage owner, and reviewer. |
| Policy exceptions | Details of the policy exceptions, such as the name, number, requester, reason, policy, control objective, state, substate, valid from, valid to, and risk rating. |
| Evidence | Details of Evidence, such as the name, number, evidence for, request reason, state, substate, requester, assigned to, and due date. |
| Entities | Details of the entities, such as the entity, description, class, and owner. |
| Controls | Details of the controls, such as the name, number, entity, function, state, status, exempt, owner, and description. |

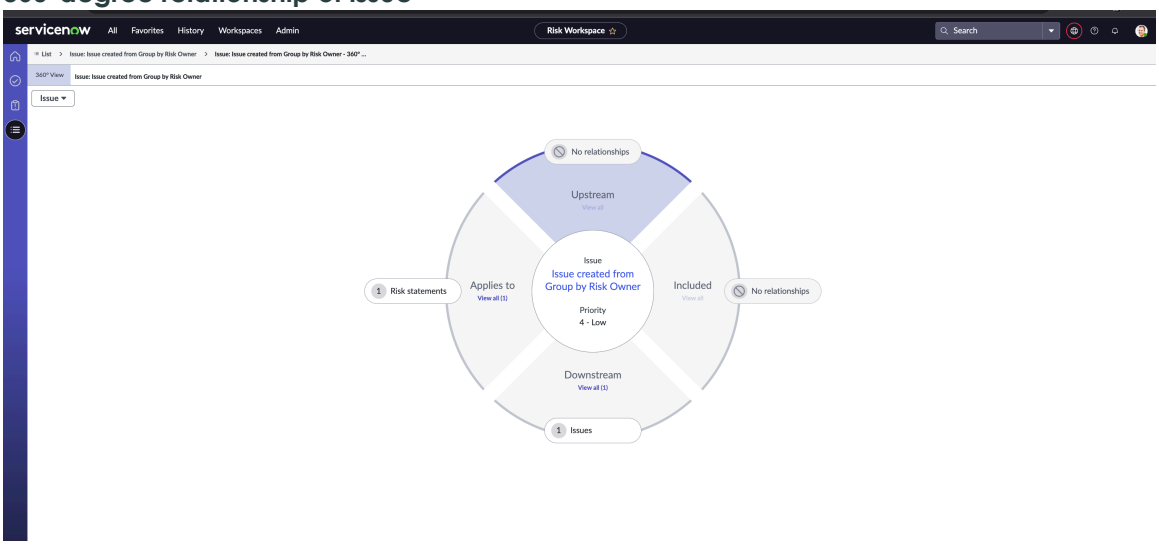
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related lists in the Issues section (continued)**

| Related lists | Description |
|---|---|
| Risks | Details of the risks, such as the name, number, entity, risk statement, owning group, owner, state, and risk assessment methodology. |
| Engagements | Details of the engagements, such as the name, number, type, engagement lead, state, engagement planned start date, and engagement planned end. |
| Control objectives | Details of the control objectives, such as the name, source ID, source, parent, category, classification, type, and compliance. |
| Risk Statements | Details of the risk statements, such as the name, framework, category, description, and appetite status. |
| Policies | Details of the policies, such as the name, type, owner, state, valid from, valid to, and compliance score. |
| Authority documents | Details of the authority documents, such as the name, common name, type, and compliance score. |
| Risk events | Details of the risk events, such as the risk event,primary entity, event type, subtype, state, date of discovery, net loss, expected loss, and non-financial impact. |
| Processing activities | Details of the processing activities, such as the processing activity, processing activity category, owner, and privacy analyst. |

The following example shows a 360-degree view of the entire relationship for a selected issue, such as the upstream issues, downstream issues, controls, and remediation tasks that are associated with the Issue.

**360-degree relationship of issue**




© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Configuring an issue relationship

If an issue isn't reusable and you know that multiple similar issues were created for different controls, risk statements, or control objectives, you can still configure the issue relationship to reuse the issue in the GRC application.

You can avoid duplicating issues by reusing the same issue. All you have to do is add it to different objects. When an issue is linked to a control or risk, it's automatically linked to the entity, control objective, or risk statement of that control or risk.

By using the **Issue Relationship Configuration** tab under the GRC Administration module, you can add an issue to different objects.

**Note:** This module is visible only if you have the workspaces installed.

To install a workspace, see Add a workspace.

You can also disable an issue relationship by stopping the automatic linking of the related objects to an issue. For more information, see Configure an issue relationship.

### Configure an issue relationship

Enable or disable an issue relationship configuration record so that you can automatically link an issue with its related objects in the GRC application.

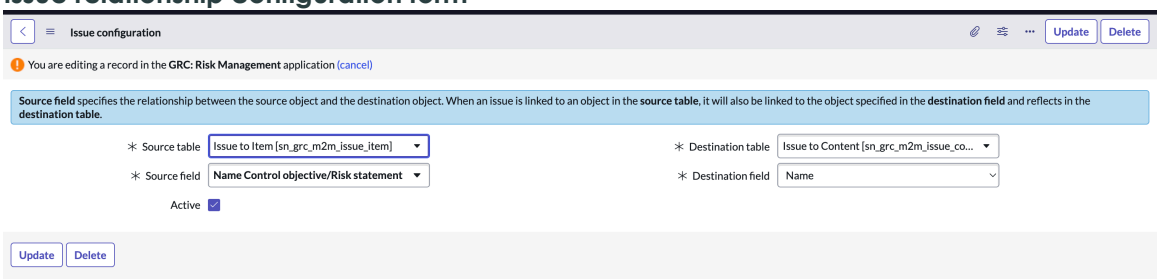
#### Before you begin

Role required: sn_grc.admin.

#### Procedure

1. Navigate to **All** > **GRC Administration** > **Issue Relationship Configurations**.
2. Select any record that you want to configure the issue relationship to.
3. Enable or disable the configuration records by selecting or deselecting the **Active** field.

**Issue relationship configuration form**




For more information about the fields in the issue relationship configuration form, see Issue Relationship Configuration form.

### Issue Relationship Configuration form

Use the Issue Relationship Configuration form in the GRC application to automatically link a destination record with an issue when it's linked to the source record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Issue Relationship Configuration form**

| Field | Description |
|---|---|
| Source table | Many to Many (MtoM) table in which the original record gets created when you link an issue to an object.<br><br>For example, if you linked an issue to a control, the relationship record is created in this table. |
| Destination table | Target table where the record is created when the issue is linked to the destination object.<br><br>For example, let's say that you selected the issue to link to a control in the **Source table** field. The issue is linked to the control's entity if you selected the issue to link to the entity MtoM in the **Destination table** field. |
| Source field | Source field that displays the relationship between the source object and the destination object. |
| Destination field | Destination field that contains the object that is linked to the issue in the **Destination table field.**<br><br>For example, if you selected the issue to link to an entity relationship in the **Destination table** field, then the destination field value is entity.<br><br>**Note:** The object types that you select in the source field and destination field should be the same types. |

**Note:**

- **Source object**: It's the original object that is linked to an issue manually.
- **Destination object**: It's the object that is automatically linked to the issue due to the issue relationship configuration.

## Domain separation in GRC

This is an overview of domain separation and the Governance, Risk, and Compliance applications. Domain separation enables you to separate data, processes, and administrative tasks into logical groupings called domains. You can control several aspects of this separation, including which users can see and access data.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Support level: Basic

- Business logic: Ensure that data goes into the proper domain for the application's service provider use cases.
- The application supports domain separation at run time. The domain separation includes separation from the user interface, cache keys, reporting, rollups, and aggregations.
- The owner of the instance must set up the application to function across multiple tenants.

Sample use case: When a service provider (SP) uses chat to respond to a tenant-customer's message, the customer must be able to see the SP's response.

For more information on support levels, see Application support for domain separation.

## Overview

Domain separation is best for those customers who:

- Need to enforce absolute data segregation between business entities (data separation).
- Customize business process definitions and user interfaces for each domain (delegated administration).
- Maintain some global processes and global reporting in a single instance.

These users can choose to expand or collapse the domain scope to show or hide data from other domains.

**Note:** Users always have access to data from domains that have been explicitly granted to them by domain visibility.

## How domain separation works in GRC

- While GRC supports separation of data, separation of logic and process is not fully supported.

- Many types of records in GRC are automatically generated through user processes. Entities, controls, risks, indicators, and control tests are all fields that can be generated automatically. For records that are automatically generated (and for any GRC record that is manually generated), the domain of the record is the same as the domain of the user responsible for creating or generating the records.

  Automatic generation should be kept in mind when working in a domain-separated GRC implementation. Users should be sure that they are creating / generating records at the right domain level so that they are visible to the right set of users.

  For example, suppose you have domains that look like:

  - Global
  - TOP
    - Domain A
    - Domain B

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- If you have a risk or control that you want to be assessed by users in domains A and B, the risk or control should be generated or manually created at the global level. If the risk or control is created in Domain B, you will not be able to recreate the risk or control in Domain A due to indexing.
- If you have a risk or control that you want to be assessed by users in TOP and Domain A, you can create the risk or control in Domain A.

Unless the risks and controls are in the Global domain, users should not assign risks or controls in a higher domain to users in a lower domain. In the example above, if you have a control in the TOP domain, you should not assign it for attestation to users in Domains A or B since those users would not have access to the control; thus the attestation or assessment questionnaire would not be generated.

Similarly, users should not assign control objectives and risk statements in a higher domain to attestations and assessments in a lower domain. Otherwise the attestation or assessment questionnaire would not be generated.

## Use case

GRC data for IT can be separated from the GRC data of other departments. Each business area using the GRC application can have separate data that cannot be shared with other departments. Therefore each department can have its own entities, policies, controls, risks, and so on.

When looking at a control from the IT domain, the user can choose to expand the domain scope to show values from the Finance domain or collapse the domain scope to show only controls that match the IT domain.

By default, domain separation adds a domain field to the Task `[task]` and Configuration Items `[cmdb_ci]` tables and their extensions.

You can extend domain separation to any new tables you create by adding a `sys_domain` field to the table's dictionary definition. By default, the system only domain-separates platform and baseline application tables where appropriate.

**Warning:** ServiceNow does not recommend domain separating platform tables (any table with the sys_ prefix such as the Dictionary Entry `[sys_dictionary]` and Dictionary Entry Override `[sys_dictionary_override]` tables) because it can produce unexpected results.

In this use case, client scripts, business rules, workflows, processes, and so on can be domain-separated.

While the behavior offered with domain separation provides multi-tenancy support, multi-tenancy is still contained within a single instance. This means that some global properties, some global data, and some global processes are shared across all domains. For example, the system's "Remember me" option on the login page is global and cannot be specified per domain.

If you need complete and total separation of all system properties and do not require global reporting or global processes, separate instances are the best option.

Related topics

Domain separation for service providers

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

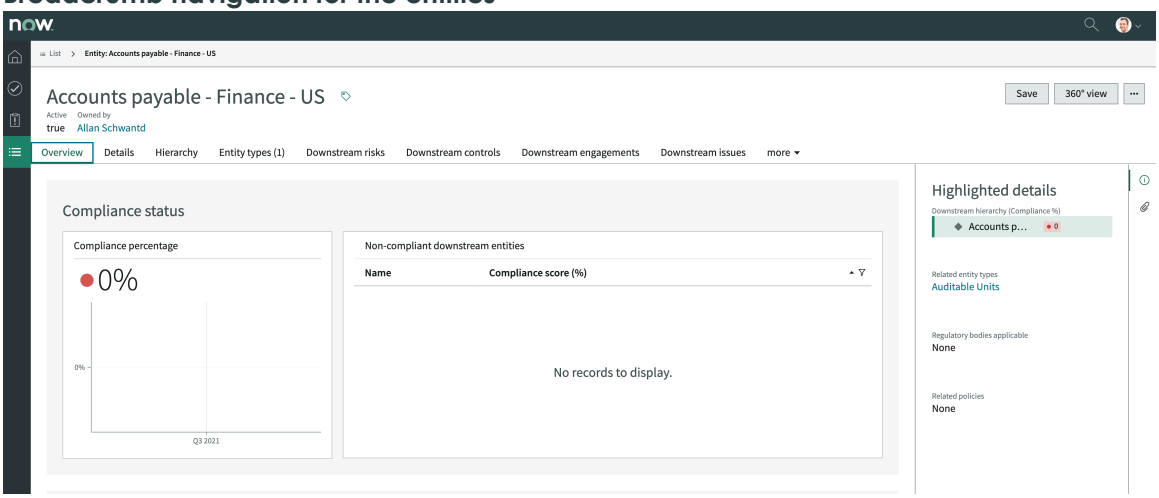
# Breadcrumb navigation

The ServiceNow® Utah release supports breadcrumb navigation for all GRC modules. Breadcrumbs provide a browser path to navigate a hierarchy of linked pages with related content.

Breadcrumbs provide context, consistency, and familiarity for the users. The breadcrumb style navigation provides a digital trail from the user's starting point to the current content, with the ability to navigate to each link. Use the breadcrumb style navigation that provides a browser path to navigate a hierarchy of linked pages with related content.

Breadcrumbs offer a quick form of filter navigation and are ordered from left to right. The left condition is the most general, and the right condition is the most specific. For example, you can see the navigation path for the Entities in the workspace view:

**Breadcrumb navigation for the entities**




The navigational path **List** > **Entity: Accounts payable-Finance-US** in the example indicates that you can navigate to the Accounts payable - Finance - US page from the Entity menu in the List view. Clicking any link in the path returns you to the selected screen.

# Taxonomy management in GRC

Taxonomy is used to organize, classify, and label the elements of the unstructured content. The content is organized into granular elements that provide more information about the context of the content.

Use the new GRC: taxonomy management application to manage categories for your content classification across GRC modules by using the Taxonomy module. In addition, you can use the GRC: taxonomy management application to store your taxonomy. The GRC: taxonomy management application is automatically installed with the GRC: Policy and Compliance Management application.

It helps to adapt and reuse the content efficiently across different segments and products. The GRC: taxonomy management application stores the taxonomy and it provides a way to map the taxonomies via a UI component for all the GRC modules.

The new GRC: taxonomy management application provides the following benefits:

- It provides a better alignment with the regulations.
- It categorizes and classifies the regulatory content easily within the GRC module.
- It sets up an internal taxonomy or maps the taxonomy from an external provider to categorize different types of library objects such as Authority documents and Citations.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- It provides the following out-of-the-box (OOTB) classification elements:
  - Content type
  - Jurisdiction
  - Regulatory body
  - Sector
  - Theme
- It offers the flexibility to add the new taxonomy categories with a new taxonomy class record in addition to the taxonomy categories provided out-of-the-box (OOTB).
- It helps you to streamline your regulatory compliance, trace the regulatory requirements, and update the external regulations.

**Note:** If you have downloaded the Regulatory Change Management application previously and you are upgrading to the Utah GA release, copy the data from the old taxonomy tables to the new taxonomy tables.

## Landing Page Configurations module

GRC administrators can now configure the Tasks and Issues overview landing pages in the workspaces by using the GRC Landing Page Configurations module in the classic user interface. The role required to configure the tasks, issues, and other items in the Landing Page Configurations module is the sn_grc_workspace.task_admin role. GRC administrators are assigned the sn_grc_workspace.task_admin role by default.

### Landing Page Configurations module

The GRC Landing Page Configurations module displays the following modules:

- Tasks Page Configuration
- Issue Page Configuration

### Tasks Page Configuration module

The Tasks Page Configuration module in the classic user interface displays the configurations related to the Tasks section in the landing pages of the workspaces. The configurations in the Tasks Page Configuration module help the users to view the data in different workspaces.

Only users with the sn_grc_workspace.task_admin role can configure the Tasks landing pages for the workspaces using the Tasks Page Configurations module in the classic user interface. The administrators are assigned the sn_grc_workspace.task_admin role by default.

GRC administrators perform task page configurations, including the workspaces, tabs, and filters configurations in this module. Based on all the filter conditions that are applied at table levels or state levels, the users can view the data in the Tasks landing page in the workspace.

In the homepage view of the workspace, the widgets displayed about the tasks such as My tasks and My group's work are configured using the UI Builder. Clicking these widgets in the homepage view directs the users to the Tasks page in the workspace.

For the Audit workspace, Compliance workspace, Privacy workspace, and Risk workspace, the following pre-configured tabs are shipped by default:

- My pending tasks
- My group's tasks

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

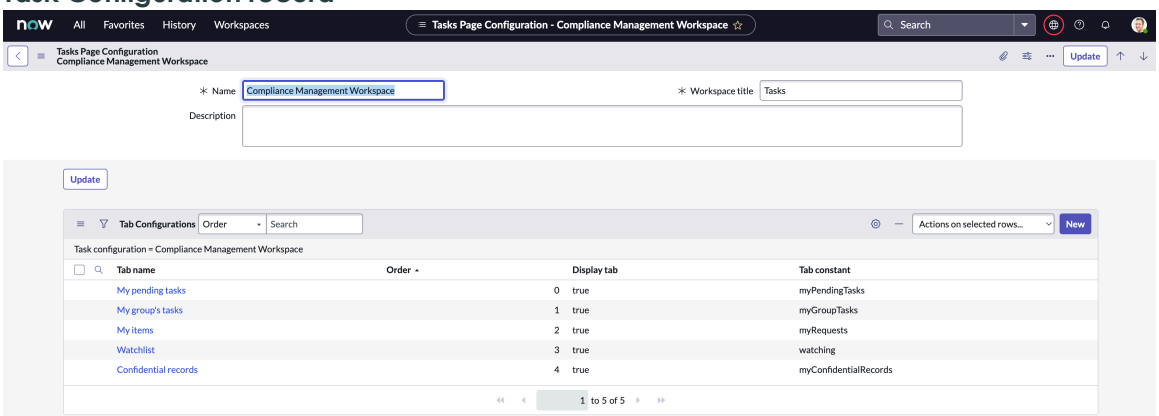
- My items
- Watchlist

Starting with GRC: Common Workspace Elements application version 14.x, the administrators with the sn_grc_workspace.task_admin role can add or remove the tabs in the Task Configuration record. They can also prioritize or order the tabs in a sequence. When a tab is created in the Task Configuration record under the Tasks Page Configuration module, it is displayed in the workspace UI.

The task administrators can change the order of the tabs in the UI. If the same order is configured for two tabs, the tabs are displayed in an alphabetical order.

The following image shows the updated Task Configuration record.

**Task Configuration record**




GRC administrators can configure the names of the task configuration records that are displayed in the landing pages. Administrators can do the following:

- Update the name and description of the record in the classic user interface. Only administrators can view this data in the classic user interface. End users cannot view this data in the workspace view.
- Update the title of the workspace that is displayed in the Tasks landing page in the workspace. End users can view this data in the workspace view.
- Update the title of the applicable table, filter condition, and column names.
- Update the filter conditions for the tabs.
- Filter the records based on the group selection for the applicable table.
- Add, update, remove, or override the state labels of the tables.
- Update the type of the tab such as group tab or regular tab.

## Update the Tasks Page Configuration record

Update the Tasks Page Configuration record in the classic user interface to display the task configurations in various workspaces. The Tasks Page Configuration record displays the configurations that an end user can view in the My Tasks landing page in each workspace.

**Before you begin**
Role required: sn_grc.admin, sn_grc_workspace.task_admin

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### About this task

GRC administrators can configure the tasks that the workspace users can view in the workspace. The following tabs are used to configure the tasks and they are provided by default for each workspace:

- My pending tasks
- My group's tasks
- My items
- Watchlist

Depending on the workspace selection, these configurable tabs are displayed in the workspace. GRC administrators can modify these tabs using the Landing Page Configurations module.

State filters or second-level filters are available for the My pending tasks, My group's tasks, My items, and Watchlist tabs.

### Procedure

1. Navigate to **All** > **GRC Landing Page Configurations** > **Tasks Page Configuration**.
   The Tasks Page Configuration record displays the configuration records for each of the following workspaces:
   - Audit Workspace
   - Compliance Workspace: Displayed under the Policy and Compliance module.
   - Operational Resilience workspace
   - Privacy Workspace
   - Regulatory Change Management Workspace: Displayed under the Policy and Compliance module.
   - Risk Workspace
   - Risk Portal
   - Vendor Management Workspace
2. Click the configuration record for the workspace that you are working in.
3. On the form, update the fields as needed.

   The tasks page configuration record for the selected workspace displays the following fields.

**Tasks Page Configuration record**

| Field | Description |
|---|---|
| Name | Name of the task configuration that is displayed in the tasks page configuration record. |
| Description | Description of the task configuration that can be updated. |
| Workspace title | Title of the My Tasks page that is displayed in the workspace. |

The **Tab Configurations** related list displays the following tabs in the Task Configuration record:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- My pending tasks
- My group's tasks
- My items
- Watchlist
- Confidential records

The following configuration fields are displayed for all the tabs in the Task Configuration record:

**Fields in the Task Configuration record**

| Field | Description |
|---|---|
| Tab name | Name of the tab that is displayed in the workspace. |
| Order | Order of the tab in the workspace. |
| Display tab | Option to display the tab in the UI. When this option is enabled, the tab is displayed in the UI. Similarly, when this option is disabled, the tab is not displayed in the UI. |
| Enable group selection | Option to select the groups in the filter. When this option is enabled, administrators can filter the records based on the group selection for the applicable table. |

The related list for each tab displays the following information:

**Related list for each tab in the Task configuration record**

| Field | Description |
|---|---|
| Applicable tables | List of the tables that are displayed in the workspace and that are shipped with the release. These tables are the records that the user can act upon based on the matching conditions.<br><br>You can create a new applicable table or click an existing applicable table from the list to update its configuration record.<br><br>◦ The table configuration record displays the fields that are related to the selected applicable table.<br>◦ The Map states related list displays the states that are applicable to the selected applicable table. You can select a state and update its filter condition so that it is correctly displayed in the tab in the workspace. |
| Applicable states | List of the states that are applicable to the tab. These states are displayed in the |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | workspace with the Overridden label column. You can configure and update the name of the state by adding the updated state name in the Overridden label column. |

4. If needed, in the Applicable tables related list, update an existing table by doing the following:

   a. Click a table to open its configuration record.

   b. Configure the **Task title**, **Table**, **Tab level filter**, and **Displayed columns** fields and click **Update**.
   The updated fields for the selected table are displayed to the end user in the workspace.

   c. Configure the name of the state by adding the updated state name in the Overridden label column.

5. Click the **My pending tasks** tab and update the configuration fields if necessary.

   The My pending tasks tab configuration displays the available configuration and the list of the tasks configured within the tab.

6. Click the **My group's tasks** tab and update the configuration fields if necessary.

   The My group's tasks tab configuration displays the list of the tasks assigned to your group.

   **Note:** You can configure the tab name for the My group's tasks tab and its associated fields similar to the My pending tasks tab.

7. Click the **My items** tab and update the fields if necessary.

   The My items tab configuration displays the list of items that are either created by you or opened by you.

   **Note:** You can configure the tab name for the My items tab and its associated fields similar to the My pending tasks tab.

8. Click **Watchlist** and update the fields if necessary.

   The My watchlist tab configuration displays the list of the tasks for which you are in the watchlist.

   **Note:** You can configure the tab name for the Watchlist tab and its associated fields similar to the My pending tasks tab.

9. Click **Confidential records** and update the configuration fields if necessary.

   The Confidential records tab configuration displays the confidential records for the selected table.

10. Click **New** in the **Tab Configurations** related list to add a new tab in the Task Configuration record.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

a. Fill in the fields on the form.

b. Click **Submit**.
The new tab is displayed in the UI with the information for the selected groups.

11. Click **Update** to update the task configuration record.

## Issue Page Configuration module

The Issue Page Configuration module displays the configurations related to the Issues overview landing pages in various workspaces. The data displayed in the Issues overview landing page is configured using the Issue Page Configurations module in the classic user interface. The Issues overview landing page includes the Issues, Issue triages, Tracking status of the issues, and Audit observations pages.

The Issues Overview Landing page is available in the following workspaces:

- Audit workspace
- Compliance workspace
- Privacy workspace
- Risk workspace

GRC administrators can configure, monitor, and report issues for an active workspace by mapping the states, filter conditions, and tables using the Issue Page Configuration module.

Based on the configurations performed in the Issue Page Configuration module, workspace users can view the data that is assigned to them in the Issues overview landing page in the workspace.

Administrators can perform the following tasks using the Issue Page Configuration module:

- Create new Issue page configurations records in the classic user interface that are displayed in the Issues overview page in the workspace.
- Configure the issues related to the tables, tracking, issue triages, and observations for the selected tables and track policy exceptions, evidence, and so on.

The homepage in each workspace displays the issues section that provides the following information:

- The My issues section displays the Issues and Triage issues sections in a number format. Issues subsection displays the details such as Assigned to, Managing, Remediation assigned, To review, Overdue. Triage issues subsection displays the details such as Assigned to and To review.
- The My group's issues section displays the Issues and Triage issues sections in a number format. Issues subsection displays the details such as Assigned to, Managing, Unassigned manager, To review, Overdue. Triage issues subsection displays the details such as Assigned to, Unassigned owner, To review, and Unassigned reviewer.
- The Watching section displays the details such as Triage issues and Remediation tasks in a number format.

## Create a new Issue Page Configuration record

Create a new issue page configuration record in the Issue Page Configuration module in the classic user interface. The Issue Page Configuration module displays the configurations related to the Issues section in the landing pages of the workspaces. The newly created issue is displayed in the Issue overview landing page in the selected workspace.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Before you begin
Role required: sn_grc.admin

### Procedure
1. Navigate to **Landing Page Configurations** > **Issue Page Configuration**.
2. Click **New**.
   The Issue page configuration record is displayed.
3. On the form, fill in the fields.

#### Issue page configuration form

| Field | Description |
|---|---|
| Name | Configurable name of the workspace. This is the name of the tab that is displayed in the workspace. |
| Issues tab | |
| Table | Name of the table used for configuring the issues that are displayed in the workspace. The **Filter** field displays the filter condition that you can configure and display the matching records. |
| Tracking tab | |
| Policy exceptions | Option to display the policy exceptions under the Tracking section in the Compliance workspace.<br>**Note:** On the Risk workspace, policy exceptions are by default not displayed. |
| Evidence requests | Option to display the evidence requests under the Tracking section in the Compliance workspace. This option is available only when the Advanced core plugin is installed in the instance. |
| Issue triage tab | |
| This tab is available only when the Advanced core plugin is installed in the instance. | |
| Show issue triages | Option to display or hide the issue triages in the workspace.<br>**Note:** For the Audit workspace, this option is inactive by default. |
| Table | Name of the table used for configuring the issue triages. |
| Filter | Filter condition that you can configure to display the matching records. |
| Observations tab | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| This tab is available only when the Advanced Audit plugin is installed in the instance. | |
| Show observations | Option to display or hide the audit observations in the workspace.<br>**Note:** This option is by default selected for the Audit workspace. |
| Table | Name of the table used for the observation. |
| Field | Filter condition that you can configure and display the matching records. |

4. Click **Submit**.

**Result**
A new Issue Page Configuration record is created.

## Link a new Issue Page Configuration record to a workspace

Create a new Issue Page Configuration record and link it from the classic user interface to the desired workspace. After linking the Issue Page Configuration record, the workspace view displays the new settings in the Issues overview landing page.

**Before you begin**
To link a new configuration to the desired workspace, you have to update the *issuePageConfigId* property for the workspace.

Role required: sn_grc.admin

**About this task**
When a new issue configuration is created and saved in the Issue Page Configurations record, it is displayed in the workspace only after linking it to the desired workspace.

**Procedure**

1. Create a new issue configuration in the Issue page configurations record.
   For instructions, see Create a new Issue Page Configuration record.
2. Copy the sys_id of the new configuration and keep note of it.
   You will later use the sys_id to update the Issue Page Configuration record.
3. Navigate to the Experiences list in the classic user interface.
4. From the UX Applications list, select the workspace where you want to integrate the change.
5. In the selected workspace, select the *issuePageConfigId* property.
6. On the issuePageConfigId property page, set the **Value** field to the sys_id of the new configuration, and click **Save**.

   **Note:** Multiple configuration records can be configured in the workspace. But only the configuration record for which the sys_id is configured in the *issuePageConfigId* property is displayed in the workspace.

**Result**
The new issue page configuration setting is displayed in the desired workspace view.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Update an Issue Page Configurations record

Update an existing Issue Page Configurations record in the classic user interface to update the issue page configurations that are displayed in the Issues overview landing page in the workspace. After modifying the configurations in the Issue Page Configuration record, the issues, issue triages, and tracking status of the issues are displayed for the users in the desired workspace.

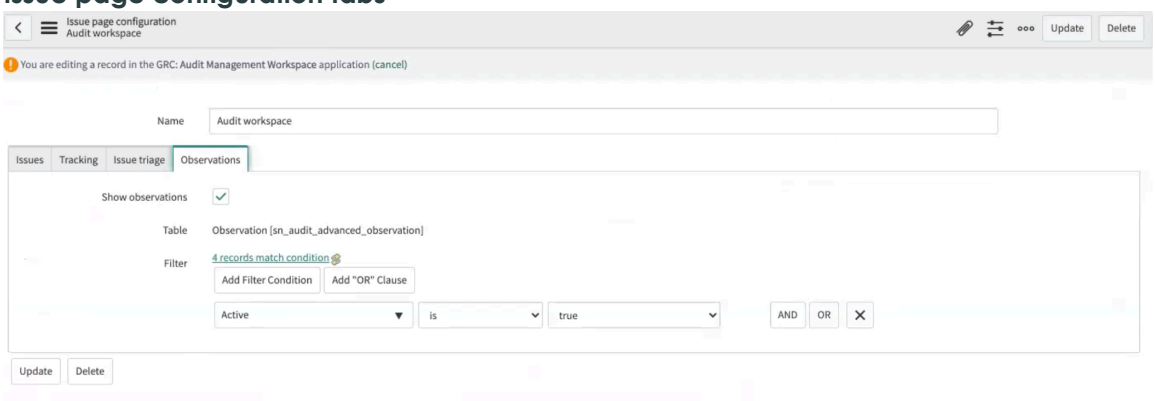
### Before you begin

Role required: sn_grc.admin

### Procedure

1. Navigate to **Landing Page Configurations** > **Issue Page Configurations**.
   The names of the available workspaces are listed in the Issue Page Configurations record.
2. Select the workspace configuration record that you want to update.
   The Issue page configuration record for the selected workspace displays a list of the tabs. You can check the filter conditions for the selected table displayed in the respective tabs and update the fields if necessary.
   - Name: Name of the tab that is displayed in the workspace.
   - Issues: Configuration to be performed to display the issues widget in the workspace.
   - Issue triage: Configuration to be performed to display the issue triage widget in the workspace.
   - Tracking: Configuration to be performed to display the Policy exceptions and Evidence requests in the workspace.
   - Observations: Configuration to be performed to display the audit observations in the workspace.

**Issue page configuration tabs**




3. In the **Issues** tab, check the filter conditions for the selected table and update the fields if necessary.
4. In the **Issue** triage tab, check the filter conditions for the selected table.
5. In the **Tracking** tab, select the **Policy exceptions** and **Evidence** options.
6. In the **Observations** tab, select the **Show observations in the Audit workspace** option, and update the filter condition.
   The page displays the name of the table for observations (sn_audit_advanced_observation) and the filter condition to be selected such as **Active is True**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Note:** The Observations widget is displayed only in the Audit workspace.

7. To update the issue page configuration record, click **Update**.

## My tasks in the workspace

GRC administrators can configure the tasks for the individual users and user groups in the GRC Landing Page Configurations module. Based on these configurations, the workspace users can view the individual user tasks, user group tasks, my items, and watchlist on the Tasks page in the workspace view.

The roles required to configure and view the workspaces are listed below.

**Roles required to configure the Tasks Page Configuration and view the Tasks page in the workspaces**

| Role | Actions associated with the role for the workspace |
|---|---|
| sn_grc.admin, sn_grc_workspace.task_admin | Configure the Tasks Page Configuration records in all the workspaces. |
| sn_grc.business_user | View the Tasks page in the Risk Portal workspace. |
| sn_audit_ws.supervisor, sn_audit_ws.auditor, | View the Tasks page in the Audit workspace. |
| sn_compliance.admin | Configure and view the Tasks page in the Compliance workspace. |
| sn_oper_res.admin | Configure and view the Tasks page in the Operational Resilience workspace. |
| sn_privacy.admin | Configure and view the Tasks page in the Privacy workspace. |
| sn_grc_reg_change.it_admin | View the Tasks page in the Compliance workspace. |
| sn_risk_workspace.IT_risk_manager and sn_risk_workspace.operational_risk_manager, | View the Tasks page in the Risk workspace. |
| sn_vdr_risk_asmt.vendor_risk_manager | View the Tasks page in the Vendor Management workspace. |

Based on the tasks that were set up by the administrators, the tasks are displayed under the following tabs in the configuration records for workspaces:

- My pending tasks
- My group's tasks
- My items
- Watchlist
- Confidential records

You can view the Tasks page in the following workspaces:

- Audit Workspace
- Operational Resilience workspace

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Policy and Compliance Workspace: Displayed under the Policy and Compliance module.
- Privacy Workspace
- Regulatory Change Management Workspace in Policy and Compliance Workspace
- Risk Workspace
- Risk Portal
- Vendor Management Workspace

**Note:** My items and Watchlist are not displayed in the Vendor Management Workspace.

## Monitor my tasks in the Tasks page in the workspace

Configure and monitor the tasks that are related to an assigned user in the workspace. Configure the landing pages and the widgets that are displayed in the workspaces using the Landing Page Configurations module. The configurations performed using the Landing Page Configurations module help you to filter the data that is displayed in different workspaces.

### Before you begin

Role required: sn_grc.admin, sn_grc_workspace.task_admin, sn_grc_workspace.task_reader

### About this task

Navigate to the individual workspaces to view the tasks, items, and watchlist for the individual users and user groups.

### Procedure

1. Navigate to the right workspace in one of the following ways:
   - **All** > **Audit** > **Audit Workspace**.
   - **All** > **Operational Resilience** > **Operational Resilience Workspace**.
   - **All** > **Policy and Compliance** > **Compliance workspace**.
   - **All** > **Privacy** > **Privacy workspace**.
   - **All** > **Regulatory Change Management** > **Compliance workspace**.
   - **All** > **Risk** > **Risk workspace**.
   - **All** > **Risk** > **Risk Portal**.
   - **All** > **Vendor Management** > **Workspace**.
2. To navigate to the Tasks page, click the tasks icon ( ).
3. Navigate to the tab that you want to view, and monitor the tasks.
   The Tasks page displays the following tabs based on the workspace configuration:
   - **My pending tasks**: Monitor the pending tasks assigned to you. The **Applicable Tables** tab under the **My pending tasks** tab on the Tasks Page Configuration module displays the list of tables that are applicable to the tasks. If the data is relevant to the user and if it matches the defined conditions, then it is populated under the **My pending task** tab in the workspace UI.

     If there is no data pertaining to you or if you do not have any assigned tasks, no data is not displayed under the **My pending tasks** tab. Only open and active tasks assigned to you are listed under the **My pending tasks** tab.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- **My group's tasks**: Monitor the tasks assigned to the user groups that you belong to. The My group's task page displays the pending tasks assigned to the user groups that you belong to. When there are no pending tasks for the user group, a message displays that All tasks are completed. Select the group from the list for which you want to filter the tasks.
- **My items**: Monitor the tasks assigned to you and the issues reported by you. The My items tab displays the list of items that are either created by you or opened by you.
- **Watchlist**: Monitor the tasks for which you are in the watchlist. The My watchlist tab configuration displays the list of the tasks for which you are in the watchlist.
- **Confidential records**: Mark sensitive records as confidential and ensure that the right people have access to these records. The Confidential records tab configuration displays the confidential records for the selected table.

**Note:** When a user or user group does not have any pending or associated tasks, a message displays under the respective tab that `All your tasks are done`.

## Exploring the entities

Entities are one of the most fundamental and crucial elements for using Governance, Risk, and Compliance. Entities can be people, processes, departments, applications, or objects that are examined for risks.

To effectively maintain the risk and compliance universe of your organization, you have to define entity types, entity classes, and entity tiers. A risk universe refers to a list of risks that your organization either faces or might face in the future. The list contains a description of each risk's criticality and frequency.

Entities are used within all offerings of GRC such as GRC: Policy and Compliance Management, Audit Management, GRC: Privacy Management and GRC: Regulatory Change Management.

### Entities in GRC

In Governance, Risk, and Compliance, entities can be people, processes, departments, applications, or objects, whose exposure must be managed. These entities have controls that are defined to view the status.

To understand entities, consider the following example. Assume you are a new GRC user and you want to implement a change management process to all your critical financial systems. All the systems can be considered as individual entities. Map all the systems to an entity class called Financial. Have an entity type filter for critical financial systems to determine the systems that are identified as critical.

The primary benefit of creating entities is that you can maintain accountability because each entity has an owner. To understand this benefit, assume that you want to configure all the servers in a new way. After you finish the configuration, you perform an audit and then discover that only one server failed to comply with the new configuration. If you had not defined all the entities, then the entire audit result would have been deemed as failed. But because you have the entities defined, then only the non-compliant server entity and its identified owner are held accountable instead of all the servers.

Having defined entities ensures that the entity owners can be identified and that appropriate controls can be applied to those entities. It also helps in tracking the entities that are non-compliant. Any entity that has child entities can be said to have downstream entities. Any entity that has parent entities can be said to have upstream entities.

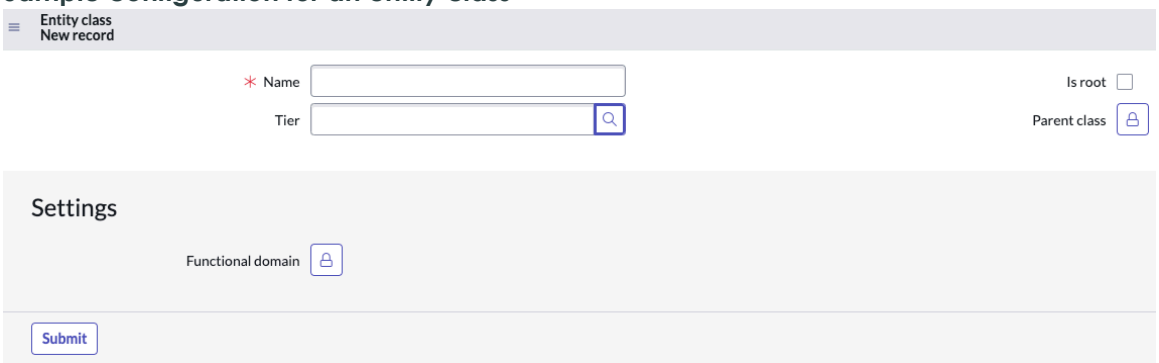
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

After creating entities, you can tag the similar entities by defining the entity class for them individually or you can link them to an existing entity class.

## Entity classes

Entity classes are used to add a conceptual information about the entity or tag the entity. To understand the concept of entity class, consider an example. A company has office branches in three cities. The office space is considered as an entity and the entity class for these entities would be the location. You can create an entity class by associating it with an entity tier as shown in the following example.

### Sample configuration for an entity class




## Entity class rules

Entity class rules help to assign classes to the entities at the table level. Any new entity created on the table gets that entity class automatically. Entity classes are used to tag your entities.

When you create an entity over a specific table, the class associated with that table automatically gets assigned to the entity. You can set a new entity class rule for a table.

## Entity types

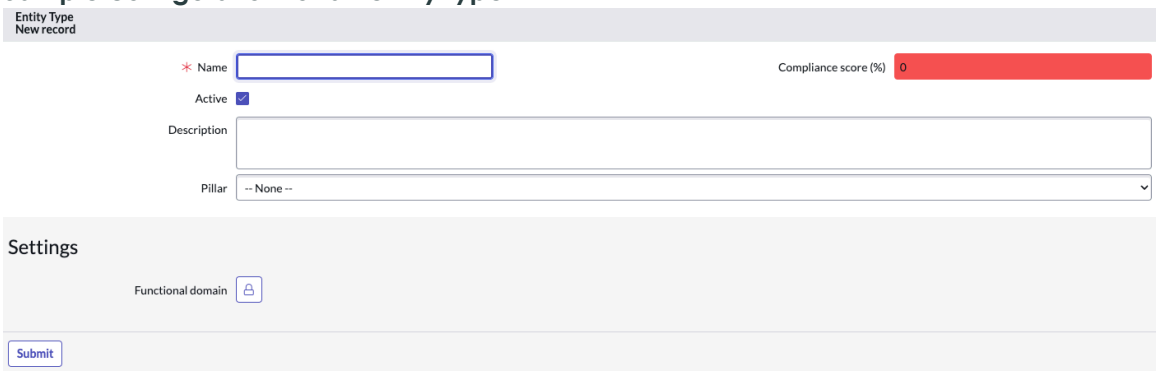
An entity type is a grouping of entities that is based on filtering. Entity types enable you to find and create entities that match a set of filter conditions. Hierarchy can be created within the entity classes.

Entity types also enable you to create risks and controls for each entity without spending much time. For example, an organization can have multiple departments, such as finance, HR, or IT. All these departments can be considered as entities and can be grouped under the entity type called Departments.

You can create an entity type by associating it with the core business pillar such as Technologies or Facilities as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Sample configuration for an entity type




## Entity tiers

When you create entity tiers, you apply a level or hierarchy to the entity classes. This level applies to all the entities in those entity classes. Entity tiers enable you to select and view the status of the most critical items in the business as shown in the following example.

### List view for an entity tier

| Name ▲ | Label | Domain | Tier level |
|---|---|---|---|
| application | Application | global | 20 |
| business | Business | global | 10 |
| it_asset | IT Asset | global | 30 |

## An entity in the workspace view

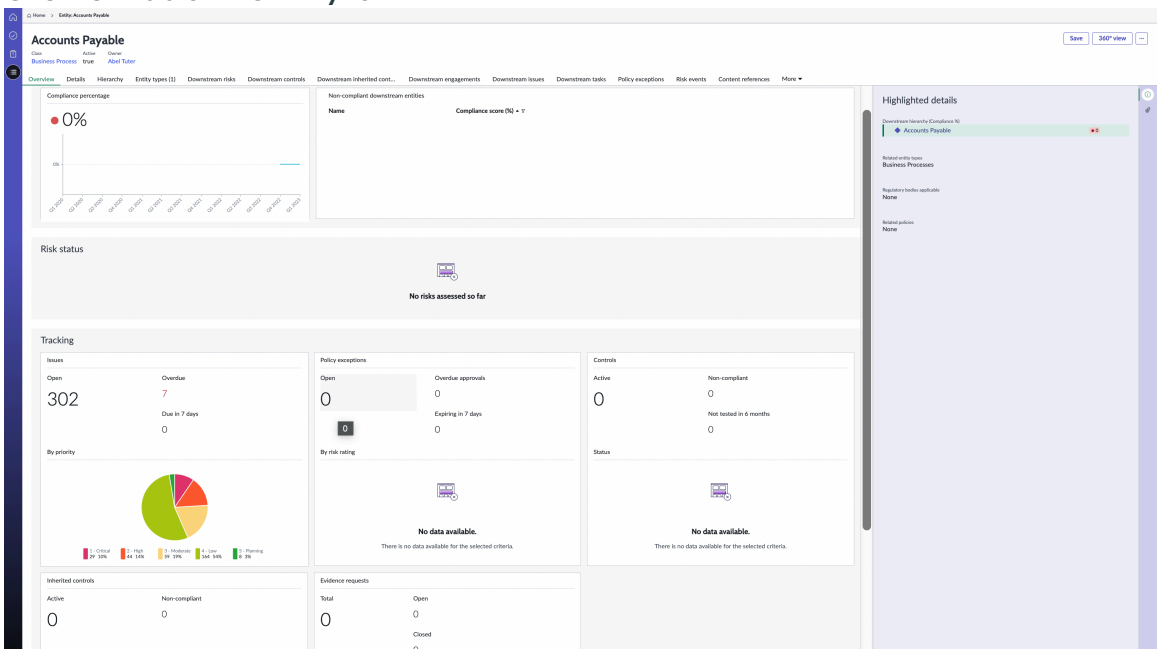
The Entity form in the workspace provides a complete view of an entity across your organization. The Entity form is listed under the Library menu of the List view in the workspace. Click an entity in the list view so that you can display its overview, details, hierarchy, entity types, or downstream risks.

## Overview details on the Entity form

The Entity form displays the details on the entity such as Compliance status, Risk status, and Tracking. The information about an entity is organized in different tabs such as Overview, Details, and Hierarchy as shown in the following example.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Overview tab on the Entity form




The related lists on the Entity form display the dependencies that are related to the entities as explained in the following table:

#### Tabs and Highlighted details on the Entity form

| Tab | Description |
|---|---|
| Details tab | Information about the entity such as Name, Active condition that shows whether the entity is active, Owned by, Class, Description, and Location information in the Entity section. The Compliance section displays the Attestation frequency such as Annually. |
| Hierarchy tab | Information about the upstream entities and downstream entities, entity class, owner information. |
| Highlighted details | Downstream hierarchy for the selected entity, related entity types, regulatory bodies applicable to the entity, and related policies. |

The Entities section displays the following related lists:

#### Related lists in the Entities section

| Related list | Description |
|---|---|
| Entity types | Details of the entity type, description, condition if the entity type was created manually and the Compliance score in percentage. |
| Downstream risks | Details of the downstream risk for the selected entity such as Number, Name, |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related lists in the Entities section (continued)**

| Related list | Description |
|---|---|
| | Entity, Class, Risk statement, Risk assessment methodology, Owning group, and Owner. |
| Downstream controls | Details of the downstream controls such as Name, Number, Entity, Control objective, State, Status, Exempt, Owner, and Description. |
| Downstream inherited controls | Details of downstream inherited controls such as Control, Number, Entity, Reliant entity, Function, State, Status, Exempt, Owner, Description, and Control objective. |
| Downstream engagements | Details of the downstream engagements such as Name, Number, Type, Parent plan, State, Engagement lead, Remaining expense budget (%), Remaining resource budget (%), and engagement planned start. |
| Downstream issues | Details of the downstream issues such as Issue, Number, Entity, Priority, Assigned to, and Issue manager. You can add existing Issues, create new issue, or remove an existing issue. |
| Downstream tasks | Details of the downstream tasks such as Name, Number, Parent, State, Assigned to, and Planned end date. |
| Policy exceptions | Details of the policy exceptions such as Name, Number, State, Substate, Policy, Control objective, Issue, Reason, Requester, Valid from, Valid to, and Risk rating. |
| Risk events | Details of the risk events such as Risk event, Primary entity, Event type, Sub type, State, Date of discovery, Net loss, Expected loss, and Non-financial impact. |
| Content references | Details of the content reference such as Content reference, Description, and version. You can click **Add** to add the content references. |
| Risk assessments | Details of the risk assessments such as Number, Risk assessment methodology, Assessable entity, Risk, Applies to record, Inherent risk, Control effectiveness, Residual risk, Response, Assessor, and End date. |
| Aggregated risks | Details of the aggregated risks such as Risk assessment methodology, Residual rating, Inherent rating, Control effectiveness, Residual ALE, Inherent ALE, Contributing risk assessments, and Risk rollup status. |

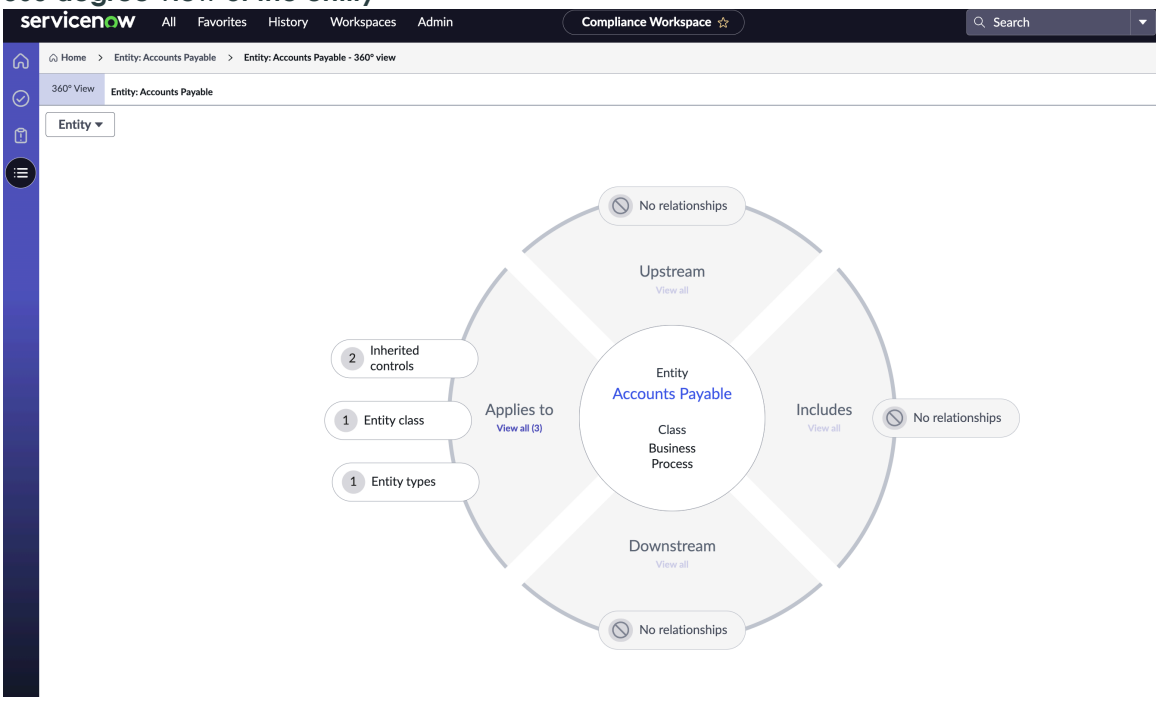
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Related lists in the Entities section (continued)

| Related list | Description |
|---|---|
| Privacy assessments | Details of the Privacy assessments such as Number, Metric type, Classification, Due date, State, and Assigned to. |

The 360° view displays an entire relationship view for the selected entity the upstream entities, downstream entities, entity class and entity type associated with the entity, and the relationships that the entity includes.

### 360 degree view of the entity




## Create an entity

Create an entity for your enterprise. In Governance, Risk, and Compliance, entities can be people, processes, departments, applications, or objects. These entities have controls that are defined to mitigate their exposure, and their audits must be completed.

### Before you begin

Roles required: sn_grc.manager, sn_risk_workspace.IT_risk_manager, and sn_risk_workspace.operational_risk_manager

### About this task

An entity is an object for an action. The entities have controls to mitigate their risk exposure. Follow this procedure to create new entities for your organization and view the downstream hierarchy, entity types, policies, and so on, related to the entity.

### Procedure

1. Navigate to the desired workspace, go to the List view, and click **Entities**.
2. To create a new entity, click **New**.
3. Navigate to the **Details** tab and fill in the fields.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Details tab in Entities record**

| Field | Description |
|---|---|
| Refers to existing record | Option that refers the new entity to an existing record. |
| Name | Name of the entity. |
| Active | Option that indicates whether the entity is active. |
| Owned by | Details of the owner of the entity such as System administrator. |
| Class | Name of the class associated with the entity such as Application or Business Entity. |
| Location | Location record of the entity with details such as address, city, state, and country. |
| Description | Description of the entity. |
| Compliance | |
| Attestation frequency | Option for attestation frequency such as daily or weekly. |

4. Under the Compliance section, add the attestation frequency such as **Weekly** or **Annually**.
5. View attachments for the entity in the side panel.
6. To save the entity, click **Save**.

> **Note:** When you create a new entity, only the **Details** tab is displayed. After the new entity is created, the **Overview** tab, **Details** tab, and other related lists are displayed.

After saving the entity, a new entity form is displayed with the Details tab, Hierarchy tab, and the following related lists:

- Entity types
- Downstream risks
- Downstream controls
- Downstream engagements
- Downstream issues
- Downstream tasks
- Policy exceptions
- Privacy assessments

For information on the fields in these related lists, see An entity in the workspace view.

7. View the highlighted details side-panel for information such as the downstream hierarchy, entity types, and policies related to the entity.
8. To save the updates to the entity, click **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Functionality enhancements for the entities

You can configure some functionality enhancements for the entities as part of the GRC updates.

The following enhancements are available for the entities:

- Email notification: When you update the entity owner value or when you assign a new owner to an entity, an email notification is sent to the entity owner about the assignment of the entity.
- Auto-update the entity owner: You can select the **Auto-update owner** option to keep the entity owner in synchronization with the value from its reference (source) field. See the following example.

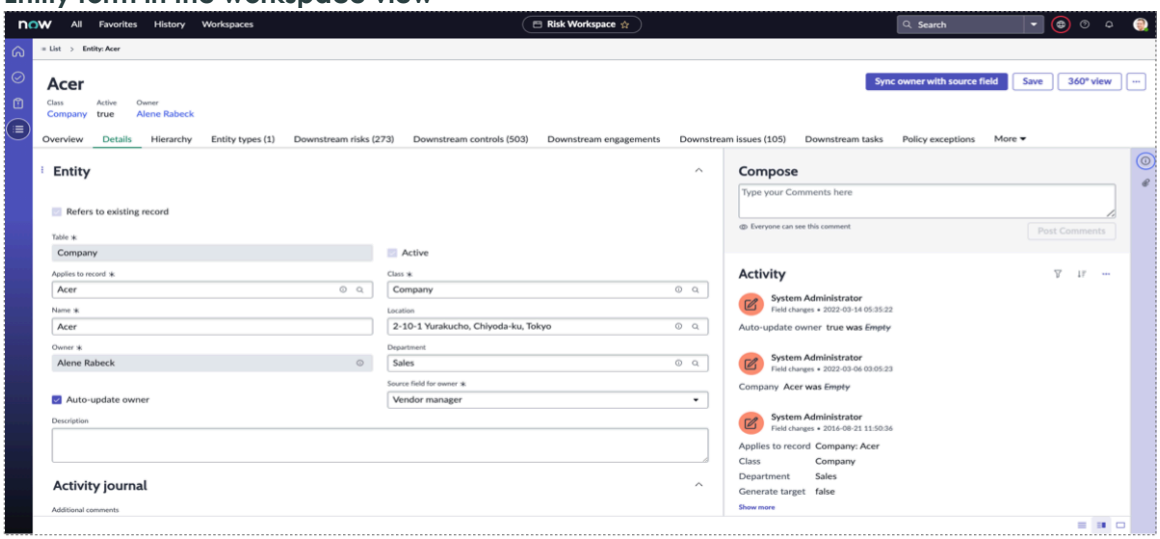
### Auto-update entity owner option




The **Auto-update owner** option is visible only for those entities that you have created by using the entity filter and that you have enabled by using the **Use owner field** option in the filter.

You can also view the **Auto-update owner** option on the entity form in the workspace view. See the following example.

### Entity form in the workspace view

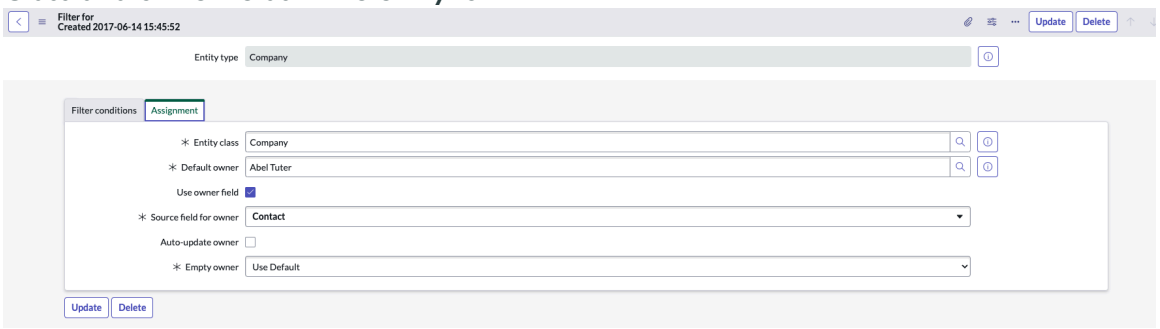



- Form design changes: The following form design changes are introduced in the entity and entity filter forms.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

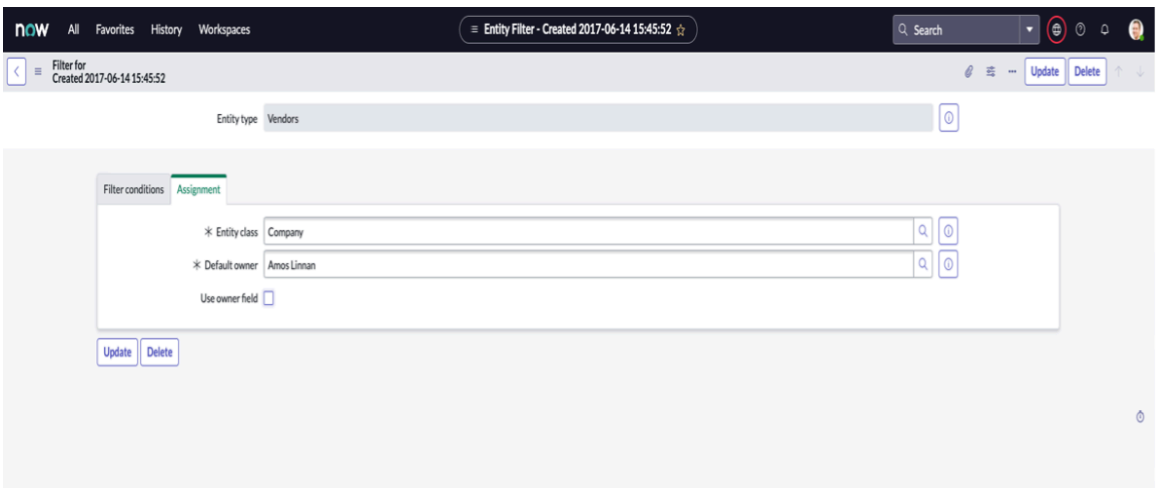
- You must fill in the **Entity class** and **Default owner** fields in the form as shown in the following example.

### Class and owner fields in the entity form




- You must fill in the **Default owner** field even if you have cleared the **Use owner field** as shown in the following example. This update ensures that every entity that has been created has an owner assigned to it.

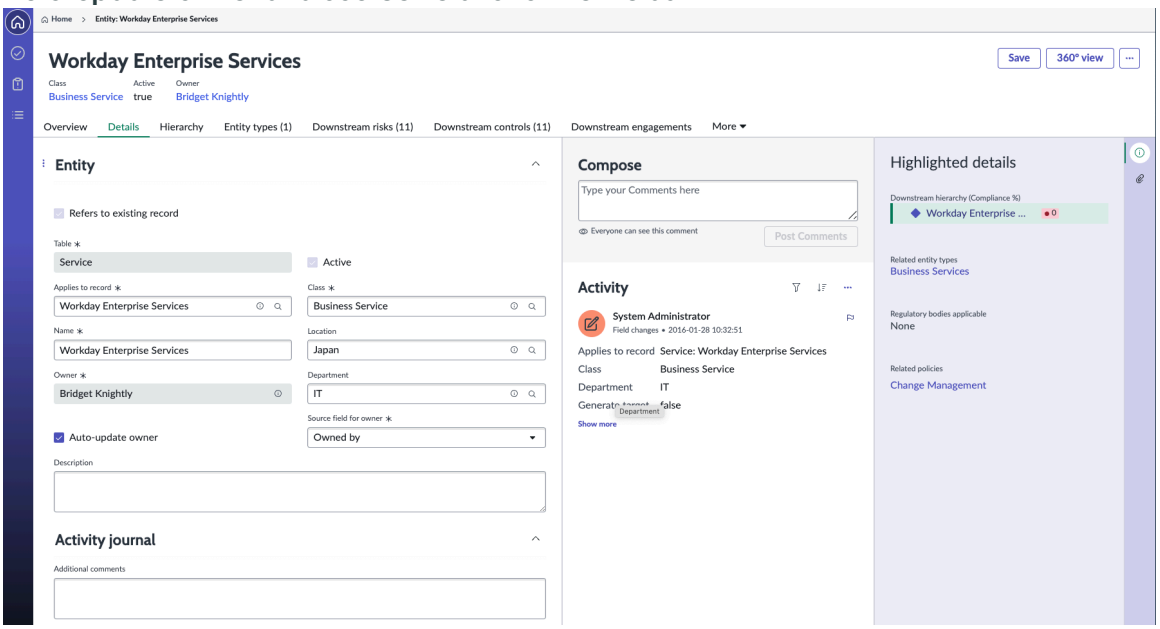
### Default owner field




- The **Department** field is added to the entity form. You can add context to an entity by selecting the department, location, and class fields.
- The **Auto-update owner** and **Source field for owner** fields are displayed in the form. The **Source field for owner** is visible only if you have enabled the **Auto-update owner** field as shown in the following example.

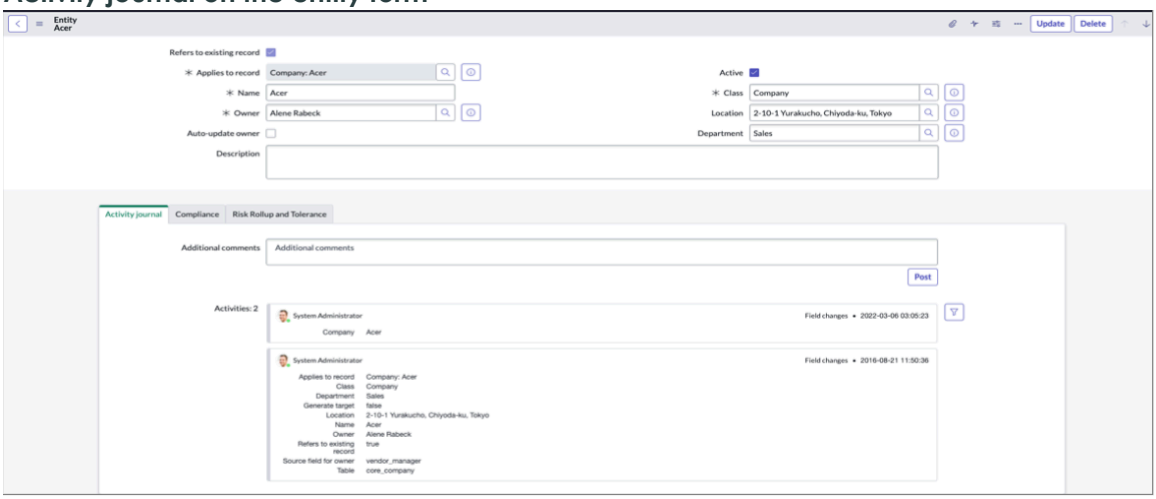
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Auto-update owner and Source field for owner fields




- The Activity journal displays the log of the changes that are made to the fields as shown in the following example.

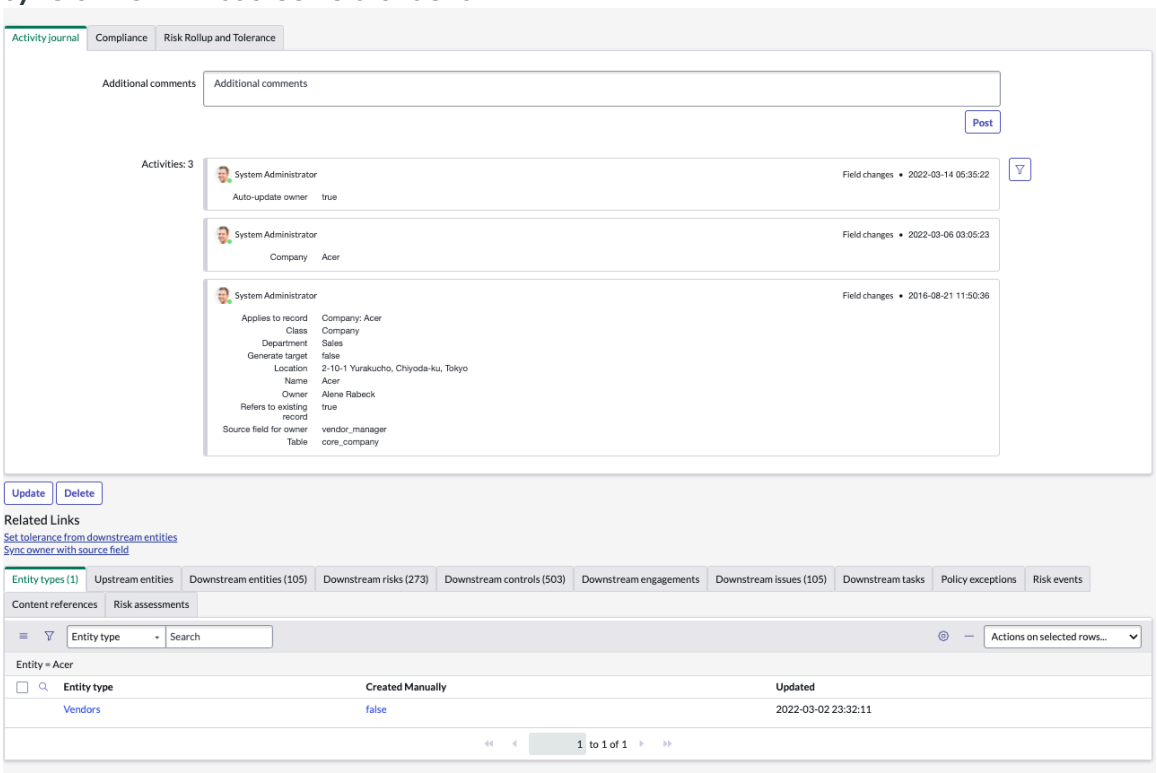
### Activity journal on the entity form




- The new **Sync owner with source field** related link is displayed in the entity form as shown in the following example. It synchronizes the owner of an entity with its source record's field value. It is visible on the form only if the value of the source field and the owner of an entity are not in synchronization.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Sync owner with source field UI action**




- You can enable the **Frequency of syncing the entity owner with the source record** property under GRC properties to synchronize the entity owner with its source record on a daily, weekly, or monthly basis.

  You can enable the **Maximum batch size while syncing the entity owner with that of its source record** property under GRC properties to set the maximum batch size to an integer value. By doing this action, you synchronize the entity owner with its source record value.

## Entity scoping in GRC

Entity scoping is permitted in each of the core GRC applications. Scoping provides a way to allocate risks and controls at different levels. Dependencies are created using the dependency map in the GRC Workbench.

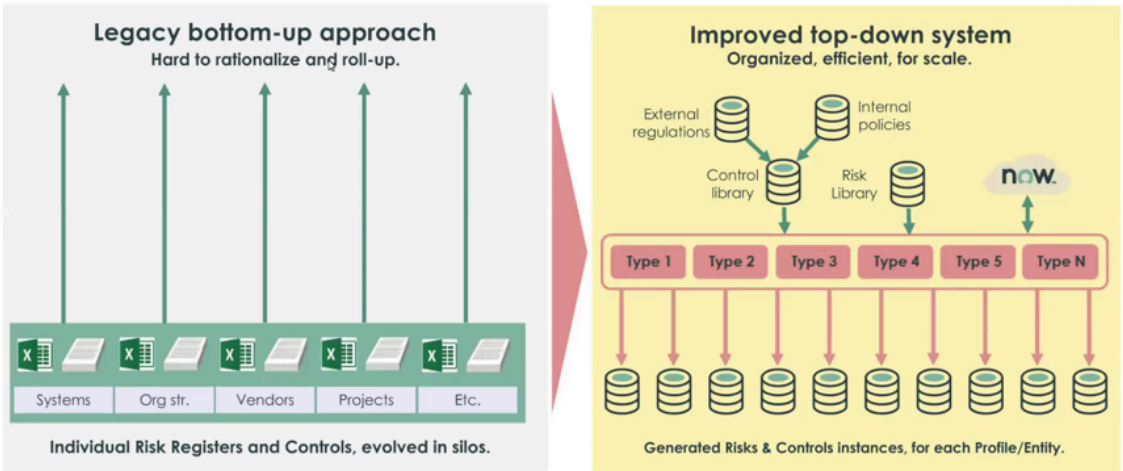
## Entity scoping overview

**Note:** Starting with the New York release, the term profile was replaced with the term entity. See GRC application nomenclature updates and industry terminology for more information about all updated GRC application terms.

Organizations have various control owners maintaining individual files and spreadsheets for tracking the compliance of different systems, projects, organizations, etc. In this environment, risk managers cannot prevent or even be aware of the duplicate risks and controls created on shared entities. The entire purpose of entity scoping is to provide a top-down approach for maintaining your risk universe, which is the hierarchical library of both risks and controls. Mature organizations with a healthy risk posture find that most risks are standard and recurring. Entity scoping helps you catalog and visualize upstream and downstream risks and controls based on the roll up of the related entities.

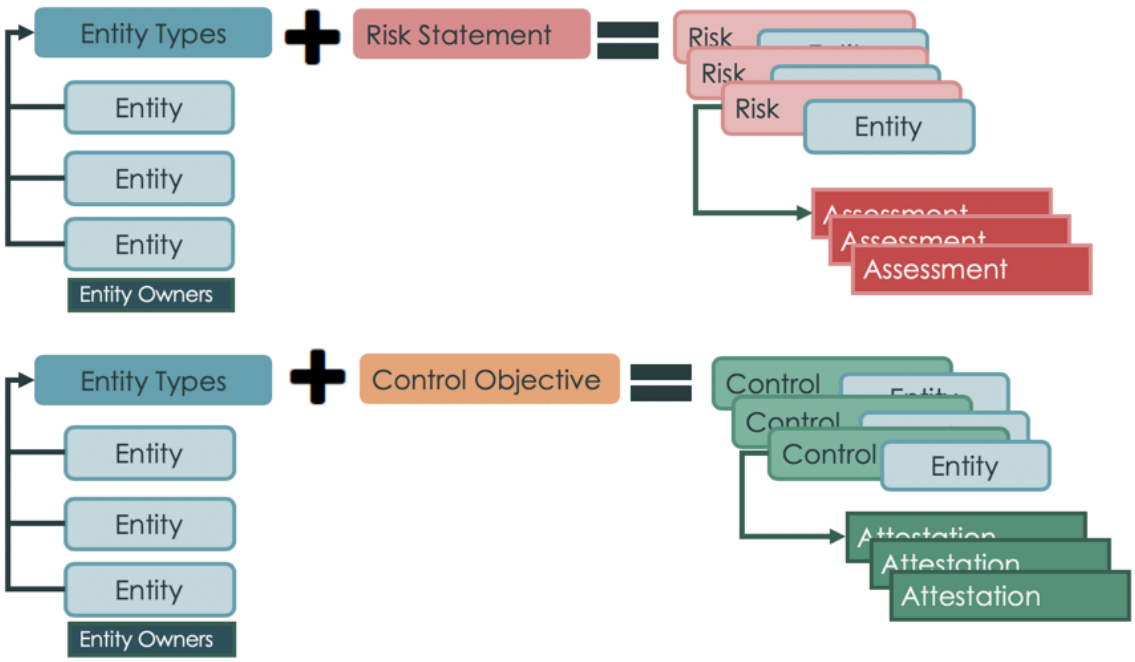
© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### From an organic approach to a structured system




1. Create or edit **Entity Types** and map them using the **Entity Filter** to existing ServiceNow® tables.
2. Map these entity types to external regulations and internal policies using control objectives and risk statements.
3. Generate risk and control instances on related entities.
4. Maintain your risk appetite and scoring results by the aggregated calculation for entities; all combos for risk scores on risk roll up.

### Scoping process




### Generate risks and controls from entity types

Create and edit entity types and map them to existing ServiceNow® tables for which you must track compliance (applications, departments, regions, processes, systems, etc.). Entities are assigned to control objectives and risk statements, which generate controls and risks for every entity type.

### Before you begin

Role required:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- sn_compliance.admin or sn_compliance.manager
- sn_risk.admin or sn_risk.manager
- sn_audit.admin or sn_audit.manager

### About this task

An entity type provides you a method to group Entities together. An entity type can be explained in the following example: Assume that you want to generate a risk of earthquake for all the data centers in a particular region. You could simply create an entity type called "Data Center" and associate all the entities of that region to the risk of earthquake based on the risk statement.

### Procedure

1. Navigate to one of the following locations.
   - **Policy and Compliance** > **Scoping** > **Entity Types**.
   - **Risk** > **Scoping** > **Entity Types**.
   - **Audit** > **Scoping** > **Entity Types**.
2. Do one of the following actions.

| Option | Description |
|---|---|
| To create a new entity type | Click **New**. |
| To edit an entity type | Open the entity type from the list. |
| To delete an entity type | Open the entity type from the list and click **Delete**.<br><br>The item generation process executes these actions in the background. With the legacy implementation of the item generation process (v1), the entity type that was marked for deletion would get deleted instantly.<br><br>With the implementation of the item generation process (v2), an entity type that is marked for deletion is not deleted instantly by the item generation process, but it is marked for deletion. When the nightly scheduled job runs, it deletes the entity type.<br><br>For more information on the item generation process, see Using the item generation process to generate controls and risks. |

3. Fill in the fields on the form, as appropriate, and click **Submit** or **Update**.

#### Entity type

| Name | Description |
|---|---|
| Name | Name of the entity type. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Name | Description |
|---|---|
| Description | Explanation of the entity type with any additional information that a user finds helpful. |

4. Once the entity type is saved, click the **Entity filters** tab and On the form, fill in the fields.

**Entity filters**

| Name | Description |
|---|---|
| Entity Type | Indicates the entity type that the filters belong to. |
| Table | Table that contains the records to be queried. |
| Filter condition | Filter conditions for the source table to generate entities. |
| Owner field | Person who owns any new entities generated from the entity type.<br>Identify the user reference field on the source table to automatically identify risk and control owners. Use default owner to assign risks to a single user when the owner field is empty. |
| Empty owner | ◦ Create<br>◦ Do not create<br>◦ Use default |

5. Click **Submit**.
6. From the **Entity type** form, click **Update Entities from Filters**.
   An informational message appears: Updating entities for this entity type.

### Create independent entities

Entities can be created manually, rather than generating them from the entity types. Entities can also be created without needing to refer to an existing ServiceNow® table, like assets, applications, business services, or processes.

#### Before you begin

Role required:

- sn_compliance.admin or sn_compliance.manager,
- n_risk.admin or sn_risk.manager
- sn_audit.admin or sn_audit.manager

#### Procedure

1. Navigate to one of the following locations:
   - **Policy and Compliance** > **Scoping** > **All Entities**.
   - **Risk** > **Scoping** > **All Entities**.
   - **Audit** > **Scoping** > **All Entities**.
2. Do one of the following actions

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Option | Description |
|---|---|
| To create a new entity | Click **New**. |
| To edit an entity | Open the entity from the list. |

3. On the Entity form, fill the fields as appropriate.

**Entity form**

| Name | Description |
|---|---|
| Refers to existing record | Select this checkbox if the entity is already part of a ServiceNow® table record. Clear this check box to create a stand-alone entity. |
| Applies to record | Select the table name and the corresponding document. This field is visible only when the **Refer to existing record**check box is selected. |
| Active | Check box to activate the entity. |
| Name | The name of the entity. |
| Compliance Score Percentage | Compliance percentage derived from Downstream controls. |
| Owned by | Select the control owner for this entity. Notifications are automatically sent to entity owners and risk managers in the event of a breach.<br>**Note:** The control owner must be a valid, active user. If an entity is assigned to an inactive user, the entity will be neglected, unless it is observed in reports. |
| Class | Entity class to which the application belongs. |
| Generate target | Select this check box if you want to create a target.<br>Every time an entity is created in the system, a target record is also created. This field is only visible if at least one of the use case accelerator applications is installed. |

4. In the Compliance related list, in the **Attestation frequency** field select the appropriate option.
This field refers to the frequency with which the attestations are sent out to the attestation respondents. The value here defaults the control frequency. If the control owner wants to have a different frequency at the control level, it can be overwritten.
5. Click Risk Rollup and Tolerance related list and fill in the form as appropriate.
This related list is visible only when Advanced Risk has been downloaded.

**Risk Rollup and Tolerance related list**

| Field | Description |
|---|---|
| Expected ALE | Annual Loss of Expectancy (ALE) refers to the product of the annual rate of occurrence (ARO) and the single loss |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | expectancy (SLE). Expected ALE is the expected value of the ALE for the risk statement. Enter currency and amount for the expected ALE.<br><br>**Note:** This value must be less than or equal to the **Maximum acceptable ALE**. |
| Maximum acceptable ALE | Threshold value for the ALE for the risk statement.<br><br>**Note:** This value must be greater than or equal to the**Expected ALE**. This value has an impact on the Tolerance status field. |
| Sum of calculated ALE | This calculation is based on the sum of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Average calculated ALE | This calculation is based on the average of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Maximum calculated ALE | This calculation is based on the maximum of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Minimum calculated ALE | This calculation is based on the minimum of calculated ALE of all the underlying risks of the risk statement and its children risk statements. |
| Tolerance Status | Automatically calculated based on tolerance values.<br><br>◦ If the **Calculated ALE** is less than or equal to the **Expected ALE** = Acceptable in green<br><br>◦ If the **Calculated ALE** is greater than the **Expected ALE**, but less than or equal to the **Max acceptable ALE** = Needs Attention in orange<br><br>◦ If the **Calculated ALE** is greater than the **Maximum acceptable ALE** = Unacceptable in red |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
| --- | --- |
| | **Note:** If the Tolerance Status changes to Needs Attention or Unacceptable, emails are automatically sent to the entity owner and risk manager to investigate. |
| Calculated Score | The corresponding score for the calculated ALE:<br>◦ Low<br>◦ Med<br>◦ High |

6. In the Basel Business Line related list, in the **Basel business lines** field, map your entity to the Basel lines of business.
7. Click **Update downstream entities business line** if you want all the downstream entities to inherit the Basel business line that you have selected.
8. Click **Submit** or **Update**.

### Relate entities to each other

Create relationships between entities to understand how controls and risks affect each other and how they affect the enterprise.

#### Before you begin

Role required:

- sn_compliance.admin or sn_compliance.manager
- sn_risk.admin or sn_risk.manager
- sn_audit.admin or sn_audit.manager

#### Procedure

1. Navigate using any of these options.
   - **Policy and Compliance** > **Scoping** > **All Entities**.
   - **Risk** > **Scoping** > **All Entities**.
   - **Audit** > **Scoping** > **All Entities**.
2. Open the entity record from the list.
3. Perform one of the following actions.

| Option | Description |
| --- | --- |
| To specify that the current entity is downstream of another entity | Click the **Add** button in the **Upstream entities** related list. |
| To specify that the current entity is upstream of another entity | Click the **Add** button in the **Downstream entities** related list. |

4. Select the desired entities to relate the current entity to and click **Create Relationship**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Result**
The entities displayed after clicking **Add** on the **Upstream entities** or **Downstream entities** related lists are limited based on the current entity's class and the tier it belongs to.

**Note:** If there are no eligible entities which can be related to the current entity, then the **Add** button is not displayed on the **Upstream entities** or **Downstream entities** related lists.

## Entity classes

Entity classes are used to add a conceptual information about the entity or to tag the entity. They are used to classify the entities and they represent a collection of entities that have the same attributes.

To understand the concept of entity class, consider an example. A company has office branches in three cities. The office space is considered as an entity and the entity class for these entities would be the location. For example, Risk as an entity could be a process or it could be the department in an organization. The entity class defines whether it belongs as a process or as a class in this example.

Entity classes are listed under Lists in the workspace view. Click an entity class in the List view to display its details.

The **Details** tab in the Entity classes form displays the following fields:

- Name
- Tier
- Parent class
- Is root check box condition

The Entity classes page displays the following related lists:

**Related lists in the Entity class form**

| Related list | Description |
|---|---|
| Entities | Information on the entities:<br>• Name<br>• Owned by<br>• Compliance Score (%) |
| Child classes | Information on the child classes:<br>• Name<br>• Tier<br>• Is root check box |

To save the newly created entity class configuration, click **Save**.

### Create an entity class

Create an entity class that is associated with an entity. Entity classes are used to add a conceptual information about the entity and classify the entities. They represent a collection

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

of entities that have the same attributes such as Department, Business Unit, or Business Service. You can gather data about the entities based on the entity class.

### Before you begin

Roles required: sn_grc.manager, sn_risk_workspace.IT_risk_manager, and sn_risk_workspace.operational_risk_manager

### About this task

Entity classes are used to classify and tag your entities. After tagging the entities, you can gather data about the entities based on the entity classes.

### Procedure

1. Navigate to the desired workspace, go to the List view, and click **Entity classes**.
2. To create a new entity class, click **New**.
3. In the **Details** tab, fill in the fields.

**Create New Entity Class form**

| Field | Description |
|---|---|
| Name | Name of the entity class. |
| Is root | Condition to check if the new entity class is a root. Options are **True** or **False**. |
| Parent class | Parent class associated with the new entity class such as Company or Department. |
| Primary risk assessment methodology | Risk assessment methodology that must be used as the primary methodology for the entity class. |
| Tier | Tier for the new entity class such as Application or Business. |
| Attachments | Attachments associated with the entity class that is displayed in the side panel. |

4. Click **Save**.
   After saving, the new entity class is displayed in the Entity classes list in the List view. When you click the new entity class, the following additional related lists are displayed:
   - Entities
   - Child classes
5. Navigate to the Entities related list and fill in the fields under the Entity class section.

**Entity class information on the Entities related list**

| Field | Description |
|---|---|
| Name | Name of the entity. |
| Owned by | Owner of the entity. |
| Compliance Score percentage | Compliance score percentage for the entity. |

6. Navigate to the Child classes related list and fill in the fields under the Entity class section.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Entity class information on the Child classes related list**

| Field | Description |
|---|---|
| Name | Name of the entity class. |
| Tier | Tier for the new entity class. |
| Is root | Condition to check if the new entity class is root. Options are True or False. |

7. To save the entity class, click **Save**.

### Update entity classes for multiple entities

Provide an entity class for multiple entities where the class field is empty. Entity classes are used to add a conceptual information about the entity and classify the entities. As an administrator, you can update the entity classes for multiple entities with a single click.

#### Before you begin

Role required: sn_grc.admin

#### About this task

The classes are only added for the entities that match the filter conditions and that do not have any entity classes associated with them. You can use the **Bulk Update Entity Class** option in the classic user interface to perform the action in the following different ways:

- **All entities with empty class**: Use this option to apply a common class to all entities that have an empty class field across all tables that match the filter criteria. As an administrator, you can set the filter conditions.
- **Select a table**: Use this option to apply a common class to all the entities that have an empty class field in the selected table.

#### Procedure

1. In the classic user interface, navigate to **Administration** > **Bulk Update Entity Class**.
2. To select your entities, do one of the following:
   - In the **Record Selection** field, select the **All entities with an empty class**.

     add the filter condition if applicable with an **ADD** or **OR** clause.
   - In the **Record Selection** field, select **Select a table** to select the entities from a table.
3. After selecting the record, click **Refresh**.
   The number of updated records that match the filter condition are displayed. The classes are added only for the entities that match the filter conditions and that do not have any classes associated with them.
4. To select the class that will be applied to the selected record, use the **Set the entity class as** field.
5. Click **Submit**.

#### Result

The entity classes for multiple entities are updated.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Scheduled jobs for GRC

Scheduled jobs are automated pieces of work that can be performed at a specific time or on a recurring schedule. GRC administrators run the scheduled jobs on demand to automate the tasks such as setting an entity class on the entities depending on the entity class rule.

Starting with the Utah release, the following scheduled jobs are provided for GRC:

- *GRC set entity class on entities based on entity class rule*: Use this scheduled job to populate the entity class rule for multiple entities at a time. The scheduled job script checks all the entity class rules, checks all the entities where the entity class field is empty, and updates the entity class for multiple entities.

- *GRC set entity class on entities same as pillar*: This scheduled job is provided for the GRC: Operational Resilience application users.

  The Operational Resilience base system includes five pillars. Pillars are the categories that are used to organize risk data that is pulled from their associated entity types. If the GRC: Operational Resilience application is installed in the instance, the **Pillar** field displays the pillar in the application to which an entity type is assigned. If an entity class is not defined for the entity type, it is mapped to the value that is displayed in the **Pillar** field using the *GRC set entity class on entities same as pillar* job.

## Entity class rules

Entity class rules help to assign classes to the entities at the table level. Any new entity created on the table gets that entity class automatically. Entity classes are used to tag your entities.

When you create an entity for a table, the class associated with that table automatically gets assigned to the entity. You can set a new rule for the entity class. Entity class rules provide the categories of the entities at the class level. The Entity class rules option is displayed under Lists in the workspace view. Click an Entity class rule to display its details.

The **Details** tab in the Entity class rules form displays the following information:

**Details tab in the Entity class rules page**

| Field | Description |
|---|---|
| Table | Name of the table that the entity class is associated with after creating an entity class rule. |
| Class | Name of the entity class to be associated with the table that uses the new entity class rule. |

## Entity class rule filter

Entity class rule filter is added in the entity class rule page to provide additional filters. Earlier, records of a table can be associated to only one entity class. Using the entity class rule filter, you can associate different classes to the records of the same table.

The **Entity class rule filter** table displays the following information:

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

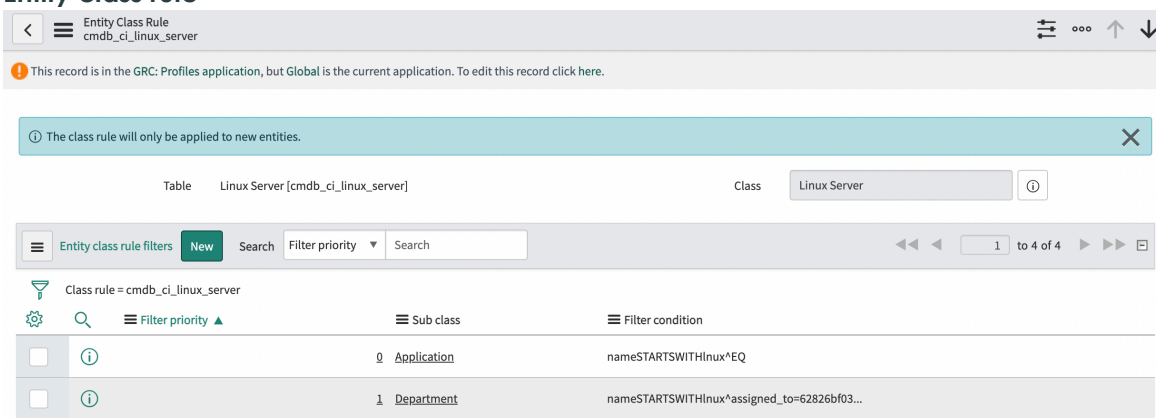
**Entity class rule filter**

| Field | Description |
|---|---|
| Filter Priority | Filter priority is the range for the subclass. The class is populated in the entity form based on the priority given. |
| Subclass | Subclass is the child class of the parent class that is displayed in the details tab of entity class rules. |
| Filter Condition | Filter Condition is used to filter out the records of the table that defines the entity class rule.<br><br>For example, if there are two subclasses with different condition then the parent class is populated instead of the subclasses.<br><br>**Note:** The subclasses are displayed in the entity forms only if they meet the same filter condition. |

## Logic for assigning entity classes

Assume that there is a record in the cmdb_ci_linux_server table and an entity class rule associated to this table. The entity class rule has these class rule filters:

**Entity class rule**




**Scenario 1**: If the entity's source record belongs to the cmdb_ci_linux_server table and matches all the conditions of the second filter, then the entity's class is auto-populated as sub class, **Department**.

**Scenario 2**: If the entity's source record belongs to the cmdb_ci_linux_server table and its name starts with lnux (satisfies both the filters), then the sub class **Application** is auto-populated as an entity class.

**Scenario 3**: If the entity's source record doesn't satisfy any of the class rule filters, then the class **Linux Server** is auto-populated as an entity class.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

### Create an entity class rule

Create a rule for an entity class. Entity class rules provide the classification of the entities at the class level. You can create a new entity class rule for an entity class that is associated with a table. After creating the new entity class rule, the Entity class rules table is updated with the new record.

#### Before you begin

Roles required: sn_grc.manager, sn_risk_workspace.IT_risk_manager, and sn_risk_workspace.operational_risk_manager

#### Procedure

1. Navigate to the desired workspace, go to the List view, and click **Entity class rules**.
2. Click **New**.
   A Create New Entity class rule page with the **Details** tab is displayed.
3. On the form, fill in the fields.

**Create entity class rule form**

| Field | Description |
|---|---|
| Table | Table that the entity class belongs to. |
| Class | Class associated with the entity such as Business unit or Application. |

4. To save the entity class rule, click **Save**.

### Create an entity class rule filter

You can create an entity class rule filter to assign classes at the filter level on the same table that is defined on the class rule.

#### Before you begin

Role required: sn_grc.manager, sn_risk_workspace.IT_risk_manager, and sn_risk_workspace.operational_risk_manager

#### Procedure

1. Navigate to the desired workspace, go to the List view, and click **Entity class rules**.
2. Select any entity class rule from the list.
3. To add a new entity class rule filter, in the **Entity class rule filters** tab, click **New**.
4. Fill in all the fields in the table.
   For more information about the fields, see Entity class rule filter fields.
5. Click **Submit**.

#### Result

A new record is created under the Entity class rule filters related list in the Entity Class Rule form.

### Entity class rule filter fields

You can create an entity class rule filter by filling out the fields that display after you click the **New** option in the entity class rule filters related list.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Entity class rule filter fields**

| Field | Description |
|---|---|
| Table | Table that is auto-filled from the associated entity class rule. |
| Subclass | Entity class to be applied for all the entities whose source record matches the class rule filter. |
| Filter condition | Condition that can filter out the records from the table. The entity class that is specified in the subclass may be applied (as per the class assignment rules) to the entity that is associated to any of these records. |
| Filter priority | Filter priority. If a source record of an entity satisfies a multiple class rule filters condition, the class is picked from the filter with the lowest priority.<br><br>For example, if you have two subclass applications and departments that have priority 0 and 1, respectively, the application subclass that has the lower priority is auto-filled in the rule and control form. |

## Entity types

Entity type is a grouping of the entities that match a set of filter conditions. You can create a hierarchy of the entity types within the entity classes. The Entity types option is displayed under the Lists view in the workspace. Click an entity type to display its details.

An entity type is a grouping of entities that is based on filtering. Entity types enable you to find and create entities that match a set of filter conditions. Hierarchy can be created within the entity classes. Entity types also enable you to create risks and controls for each entity without spending much time. For example, an organization can have multiple departments, such as finance, HR, or IT. All these departments can be considered as entities and can be grouped under the entity type called Departments.

Within an entity type, you can assign an owner and an entity class. You can associate a control objective and risk statements to the entity type so that risks and controls get automatically created for those entities. For every entity created using the entity type, the configuration and filter are applied so that the entity class and entity owner get automatically assigned for each entity.

When you create entity types and associate risk statements and control objectives to them, the risk and controls are automatically created for all the entities. The benefit of creating entity types is that it eliminates the need for maintaining multiple spreadsheets with the associated risks and controls for each entity. By applying entity types, you can quickly create entities by using the entity filters that are present within the entity types. Entity types can contain entities associated with different classes.

Grouping entities also helps in rolling up and aggregating the risk scores after risk assessments are performed. To understand how grouping entities contribute to rolling up the risk scores,

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

consider the following example. Assume that there's a banking organization called Acer Finance. Acer Finance has two business lines: Banking and Retail. The Banking division has further subdivisions such as Commercial Banking and Private Banking. The risk assessments are generally performed at the bottom-most level. In this example, the assessment is performed at the Commercial Banking and Private Banking levels. The reporting, however, is done at the top-most level. This means that the risk assessment scores of Commercial Banking and Private Banking roll up and aggregate at the Banking level. Similarly, the scores of the Banking and Investment roll up to the Acer Finance organization level.

Entities in entity type are created based on the conditions set in the Entity Filter. In entity filters, the following filter conditions are defined:

- Build your own conditions: The entity filter defines the table from which the data is pulled into each entity type for display. Options in the Entity filter related list under Entity Type are revised such that **Build your own conditions** is same as the previous condition builder.
- Select from predefined queries: A new option is introduced as **Select from predefined queries** that uses the Configuration Management Database (CMDB) queries.

The Details tab in the Entity type page displays the following information:

- Name
- Compliance Score (%)
- Check box condition to display if the entity type is active
- Description

The Entity type page displays the following related lists:

**Related lists in the Entity type section**

| Related list | Description |
|---|---|
| Entities | Information on the entities:<br>• Entity<br>• Description<br>• Class<br>• Owned by<br>• Residual rating<br>• Compliance Score (%) |
| Entity Filters | Information on the entity filters:<br>• Entity filter type<br>• Table<br>• Filter condition<br>• Use owner field<br>• Owner field |
| Risk frameworks | Details of the risk framework. Click **Add** to add a new risk frameworks record. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

**Related lists in the Entity type section (continued)**

| Related list | Description |
|---|---|
| Risk Statements | Details of the risk statements such as Risk Statement, Framework, Category, and Description. |
| Policies | Details of the policies such as number, name, Type, Owner, State, Valid from, Valid to, and Compliance Score percentage. |
| Control Objectives | Details of the control objectives such as Control objective, Category, Type, Classification, and Compliance Score percentage. |
| Entity Filters | Details of the entity filter such as Entity Filter type, Table, Filter Condition, Query, Information objects, Use owner field, Owner field. |
| Policy Exceptions | Details of the policy exceptions. |
| Content References | Details of the content references. |
| Privacy assessments | Details of the privacy assessments for the entity type. |
| Attachments | Attachments associated with the entity type displayed in the side panel. |

### Create an entity type

Create an entity type for the entities in your system. Entity types enable you to find and create new entities that match a set of filter conditions. You can create a hierarchy of the entity types within the entity classes.

## Before you begin

Roles required: sn_grc.manager, sn_risk_workspace.IT_risk_manager, and sn_risk_workspace.operational_risk_manager

## Procedure

1. Navigate to the desired workspace, go to the List view, and click **Entity types**.
2. Click **New**.
   A Create New Entity Type page with the **Details** tab is displayed.
3. In the **Details** tab, fill in the fields.

**Details tab in the Create New Entity Type page**

| Field | Description |
|---|---|
| Name | Name of the entity type. |
| Compliance Score Percentage | Compliance score percentage assigned to the entity type. |
| Active | Option to set the entity type as active. |
| Description | Description of the entity type. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

4. To save the entity type, click **Save**.
   When you save the entity type, the other related lists are displayed on the Entity type page. Update the related lists as applicable.
   - Details
   - Entities
   - Entity Filters
   - Risk Frameworks
   - Risk Statements
   - Policies
   - Control Objectives
   - Policy Exceptions
   - Content References
   - Privacy Assessments

   See An entity in the workspace view for more information.

5. To save the entity type, click **Save**.

### Entity filters

Entity types enable you to find and create entities that match a set of filter conditions. Entity types include predefined entity filters that define the data to be displayed in the user interface. The entity filter defines the table from which data is pulled into each entity type for display.

Entities in entity type are created based on the conditions set in the entity filter. You can create a new entity filter by navigating to the Entity types tab under the List view.

The options in the **Entity filter** tab under the Entity type are revised so that **Build your own conditions** condition builder uses the same option that was used in the previous condition builder. In addition, the new **Select from predefined queries** option leverages the Configuration Management Database (CMDB) queries. The following options are now available in the Entity filters related list under Entity type:

- Build your own conditions.
- Select from predefined queries using the Configuration Management Database (CMDB) Query Builder.

The **Entity filters** tab displays the following information:

- Entity filter type: Entity filter type such as Build your own conditions or Select from predefined queries.
- Table: Table that contains the records to be queried such as sn_audit_advanced_auditable_unit.
- Filter condition: Filter conditions for the source table to generate entities.
- Use owner field: Use the default owner to assign risks to a single user when the owner field is empty.
- Owner field: Person who owns any new entities generated from the entity type. Identify the user reference field on the source table to automatically identify risk and control owners.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use the new Entity class field in the entity filters under the entity type to assign an entity class to an entity filter. When you use an entity filter to create an entity, an entity class gets assigned to it automatically.

### Create an entity filter

Create an entity filter under an entity type in the workspace view. Entities in entity type are created based on the conditions set in the Entity Filter. The entity filter defines the table from which data is pulled into each entity type for display.

## Before you begin

Roles required: sn_grc.manager, sn_risk_workspace.IT_risk_manager, and sn_risk_workspace.operational_risk_manager

## About this task

You can use one of the following filter conditions for the entity type:

- Build your own conditions
- Select from predefined queries

## Procedure

1. Navigate to the desired workspace, go to the List view, and click **Entity types**.
2. Click an entity type in the list and navigate to the **Entity Filters** tab.
3. To create a new entity filter, click **New**.
   The Create New Entity Filter page is displayed.
4. In the **Details** tab, fill in the fields.

**Create New Entity Filter form in the Details tab**

| Field | Description |
|---|---|
| Filter for | |
| Entity type | Name of the entity type under which the new entity filter is created. |
| Filter conditions | |
| Entity filter type: **Build your own conditions** | Type of the entity filter that is used for filtering the data. Use the Configuration Management Database (CMDB) Query Builder to build your own query.<br><br>The Configuration Management Database (CMDB) is used to search the database for the entities. It provides the following methods for filtering:<br><br>◦ **Build your own conditions**<br>◦ **Select from predefined queries**<br><br>Complete the following steps for the **Build your own conditions** entity filter type:<br><br>**a.** In the **Entity filter type** field, select the entity filter type as **Build your own conditions**.<br><br>**b.** In the **Table** field, select a table from the populated list.<br><br>**c.** In the **Filter condition** field, click **Set conditions**, build a filter condition, click **Set**, and view the matching results. |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Entity filter type: **Select from predefined queries** option | Predefined query to scope the entity. Complete the following steps for the **Select from predefined queries** option:<br>**a.** In the **Query** field, select a predefined query such as **Business Apps using Information Object** that is applicable for the selected entity.<br>Table associated with the entity when a predefined query is selected. The table is automatically populated.<br>**b.** In the **Information objects** field, select only the applications and processes that have information objects associated with them. To add more information objects, click **Information objects** and type information objects such as `Email`.<br>**Note:** To use a predefined CMDB query for entity scoping, GRC administrators must assign the **GRC Scoping** tag to the selected CMDB query.<br>As a sn_grc.admin user, navigate to **Policy and Compliance > Administration > GRC Properties** or navigate to **Risk Administration > GRC Properties** in an instance, set the **Enable entity scoping for CMDB query** property as **Yes** and click **Save**.<br>The Information object to entity mapping using CMDB query is available on the Utah platform from Utah patch 3 release only. |
| Assignment | |
| Entity class | Entity class to be associated with the entity type. You can now assign an entity class to an entity filter under entity type. When a new entity gets created using an entity filter, an entity class gets assigned to it automatically. |
| Use owner field | Option to use the owner field. Owner field will be applied as owner for the entities created from the filter. This condition uses the **Owner** field information in the query. When the check box for this field is selected, the following fields are displayed:<br>◦ **Owner** field: Select the owner to be associated with the new entity generated by the filter.<br>◦ **Default owner** field: Select a default owner from the list.<br>◦ **Empty owner** field: Select one of the following options:<br>▪ **Do not create**: When you select this value, it will skip the creation of entity record.<br>▪ **Use Default**: When you select this value, a new field- Default Owner is shown. The value selected in Default owner field will be applied as owner for the entities created from the filter. |
| Attachments | Attachments associated with the entity that are displayed in the side panel. |

**5.** To save the entity filter, click **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Create an entity filter in the classic user interface

Create an entity filter under an entity type in the classic user interface. The entity filter defines the table from which data is pulled into each entity type for display. If the entities belong to an application, the users who have access to the entity class that is associated with the entity can only view those entities.

### Before you begin

Role required: sn_grc.manager

### Procedure

1. In the classic user interface, navigate to the **Entity types** list.
2. Click an entity type in the list and navigate to the **Entity Filters** tab.
3. To create a new entity filter, click **New**.

#### Create entity filter form

| Field | Description |
|---|---|
| Entity type | Name of the entity type. |
| Entity filter type | Type of the entity filter. The options are as follows:<br>◦ **Build your own conditions**<br>◦ **Select from predefined queries** |
| Table | Name of the table from which the records are filtered. |
| Filter condition | Filter conditions that display the matching results. |
| Entity class | Entity class for the entity type. |
| Use owner field | Option to use **Owner** field information in the query. The owner is the identified risk owner associated with the entity type. When this option is selected, the following fields are displayed:<br>◦ **Owner** field: Select a table before modifying the Owner field. Then, select the owner to be associated with the new entity filter.<br>◦ **Default owner** field: Select a default owner from the list.<br>◦ **Empty owner** field: Select one of the following options:<br>▪ **Create**: Create an owner for the entity filter.<br>▪ **Do not create**: Do not create a new owner for the entity filter.<br>▪ **Use Default**: Use the default owner for the entity filter. |

4. To save the entity filter, click **Submit**.

## Entity tiers

When you create entity tiers, you can apply a level or hierarchy to the entity classes. This level applies to all the entities that are associated with the entity classes. Entity tiers enable you to select and view the status of the most critical items in the business.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Consider the following example. Assume that the Chief Product Officer of your organization wants to see the status of only the most critical financial business applications. If you have created a hierarchy or set of tiers for the entities, then you can filter the tier 1 entities and present the required data. Each entity class can belong to only one tier.

By creating entity tiers, you can better understand how your lower tier entities affect your higher tier entities. For example, assume that you created the entity hierarchy where Business is tier 1, Application is tier 2, and IT asset is tier 3. Therefore, the risks of the entities of tier 3 affect the entities of tier 2 and that in turn affects tier 1. This roll-up or aggregation provides accurate risk scores.

The Entity tiers option is displayed under the Lists view in the workspace. Click an entity tier to display its details. The **Details** tab in the Entity tiers page displays the following information:

**Details tab in the Entity tiers page**

| Field | Description |
|---|---|
| Label | Label of the entity tier that is displayed in the user interface such as Application or Business. |
| Tier level | Tier level of the entity tier such as 15 or 20. |
| Name | Name of the entity tier such as application or business. |

### Create an entity tier

Create an entity tier for the entity classes in your organization. When you create entity tiers, you can apply a level or hierarchy to the entity classes. The hierarchy level applies to all the entities associated with the entity classes.

### Before you begin

Roles required: sn_grc.manager, sn_risk_workspace.IT_risk_manager, and sn_risk_workspace.operational_risk_manager

### Procedure

1. Navigate to the **Entity set up** > **Entity tiers** menu in the workspace view.
   The Entity tiers list is displayed.
2. Click **New**.
   A Create New Entity Tier page with the **Details** tab is displayed. The breadcrumb navigation menu is displayed at the top of the page.
3. In the **Details** tab, fill in the fields.

**Details tab in the Entity tier form**

| Field | Description |
|---|---|
| Label | Label for the new entity tier. |
| Tier level | Tier level for the new entity tier. |
| Name | Name of the new entity tier. |
| Attachments | Attachments associated with the entity displayed in the side panel. |

4. To save the entity tier, click **Save**.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

# Viewing and updating Governance, Risk, and Compliance exceptions

Report exceptions as it is critical for businesses to quickly identify and address key business process issues before they become a problem. Using exceptions to manage errors has advantages over traditional error-management techniques.

### Before you begin

Role required: sn_grc.admin

### About this task

An exception report is a document that lists instances in which actual performance is deviated from expectations. GRC exception is a capability using which you can record or associate business exceptions with GRC objects such as citations, automated factors, and so on. Each exception record has details such as the category of the exception, the record in the table, and the field with which the exception is associated. The administrator can view the list of exceptions and resolve them. Whenever an exception is raised, the solution to resolve the exception is also given in the exception description. The administrator uses the proposed solution to resolve the exception. An example of an exception is when a user has not configured a risk assessment methodology but is trying to perform an object assessment. When an administrator resolves one type of exception, all other similar exceptions get resolved.

### Procedure

1. Navigate to **GRC Exceptions** > **Exception Report**.
2. Open the exception record you want to resolve.
3. On the form, fill in the field.

**Exception form**

| Field | Description |
|---|---|
| Number | Unique number of the exception that is raised. |
| Exception category | Category to which an exception belongs. The choices are:<br>◦ Configuration: Example: A risk administrator tries configuring a form and giving a user the authority to perform a task for which the user does not have the right role.<br>◦ Runtime: Example: When something runs automatically such as an Indicator. |
| State | State of exception. The default state is **Open**. |
| Application | Application to which the exception belongs. |
| Description | Detailed description of the exception and the possible solution for resolution. |
| Exception Record Details | |

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

| Field | Description |
|---|---|
| Source table | Table on which the exception has occurred. |
| Record reference | Record on which the exception has occurred. For example, an exception is raised on a risk assessment instance response. |
| Column reference | The column that contains the record. |
| Activity | |
| Additional comments | Notes on the resolution of the exception or any other additional information. |
| Activities | Displays the stream of activities on the exception. |

4. Click **Update** after you change the state of the exception.
5. Click **Delete** to delete the record.

## Advanced Governance, Risk, and Compliance Application Risk dashboard

The GRC **Application Risk and Compliance Overview Dashboard** provides the latest view of risk and compliance aspects for the business applications that are used in an enterprise.

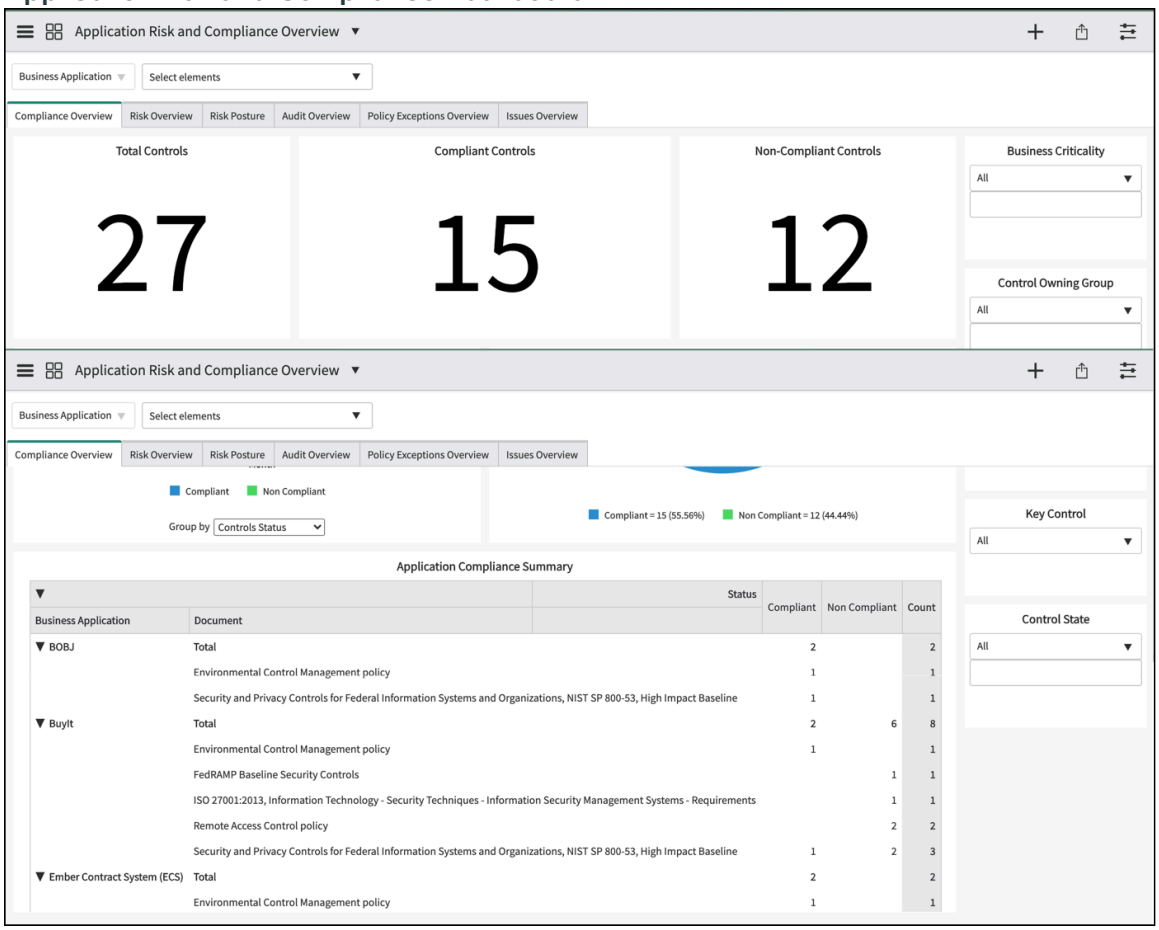
The Application Risk Dashboard is useful for the Chief Information Officer (CIO) and application owners. Both these users must have the sn_compliance.reader, sn_risk.reader, and sn_audit.user roles to view the dashboard. Navigate to **Advanced GRC Dashboard** > **Application Risk Dashboard**. The **Application Risk and Compliance Overview Dashboard** is displayed.

**Note:** To be able to view this dashboard, you must activate the GRC: Advanced Dashboards (com.sn_grc_pa_advanced) plugin and the GRC: Policy and Compliance Management (sn_compliance) plugin.

The Application Risk and Compliance Overview dashboard provides you a detailed report of the risk and compliance posture of all the business applications in an organization.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

## Application Risk and Compliance Dashboard




This dashboard highlights the following:

- The compliance impact of applications in use.
- The risk posture of applications.
- The state of remediation and exceptions activity of the issues.
- The audit activity around applications and status.

This dashboard provides answers to the following questions that are of interest to the CIO and the application owner:

1. What are the key applications, and are they all operational and delivering the required services optimally?
2. What are the policies and authority documents that the applications must be compliant to? Are the applications compliant to them?
3. What are the risks faced by the applications? Are any of them high to raise a concern? Are there enough mitigations in place? Are there adequate controls in place and are they working effectively?
4. For applications that need remediation, are the remediations being done on time according to the Service Level Agreements (SLAs)? Which are the applications that generate the maximum number of issues?
5. Are exceptions being sought often on the applications and why? Are they within manageable limits?
6. Are the applications due for audit any time? How have the applications performed on these audits?

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The dashboard offers various representations such as bar graphs, donut charts, and trend charts. Application owners can use various filters on the dashboard to view reports related to the business applications they own such as, critical business applications, mandated controls related to specific business application, or high priority issues and so on.

## Compliance Overview

The Compliance Overview tab appears when you activate the Policy and Compliance plugin. The Compliance Overview tab provides an overview of the compliance posture of the business applications and displays the following reports:

- Total Controls: This report provides the total number of active controls.
- Compliant Controls: This report provides the total number of compliant controls which are not in draft or retired state.
- Non-Compliant Controls: This report provides the total number of non-compliant controls which are not in draft or retired state.
- Compliance Status By Month: This report provides the number of active controls by month.

  **Note:** This bar chart shows the compliance status for the current month and can be grouped by either Control Status or Business Application.

- Compliance %: This report provides the percentage of different statuses of active controls such as Compliant, Non Compliant, and Not Applicable.
- Application Compliance Summary: This report provides the summary of policies, authority documents, and the controls associated with business applications.

The following filters can be used to filter data on the reports:

- Business Application
- Business Criticality
- Entity Owner
- Enforcement such as mandatory or voluntary controls
- Key Control
- Control State
- Control Owning Group

## Risk Overview

The Risk Overview tab appears when you activate the Advanced Risk plugin. The Risk Overview tab provides an overview of the risks associated with business applications and displays the following reports:

- Risk Heatmap by Application Criticality: This report displays the heatmap of the application risks based on criticality of applications versus the risk rating of the application.
- Risk Response Tasks Overview: This report displays the response tasks created for a risk and different states of those tasks.

  **Note:** This bar chart can be grouped by and stacked by risk response, risk response state, risk calculated score, risk response assigned to, or business application.

- Application Risk Summary: This report displays the summary of risks directly associated with the applications that contribute to the overall risk rating of the application. Other

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

downstream risks that contribute to the application risk rating are not represented in this report. The risks considered for this report are very high, high, and moderate.

- Application Risk Mitigating Controls Status: This report provides the information for an application's risks and the associated controls. The risks considered for this report are very high, high, and moderate. The state of controls must not be in draft or retired. The risks for only one year are displayed.

The following filters can be used to filter data on the reports:

- Business Application
- Criticality
- Risk Rating
- Application Owner
- Business Owner

## Risk Posture

The Risk Posture tab appears when you activate the Risk plugin. The Risk Posture tab provides information about the risk exposure of business applications. The reports in this tab can also be filtered using the Business Application filter. The Risk Posture tab displays the following:

- Very High Risks: This report displays the very high risks of an application.
- High Risks: This report displays the high risks of an application.
- Moderate Risks: This report displays the moderate risks of an application.
- Acceptance Task Expirations: This report displays the risk response acceptance tasks that have an expiration on the current day, the current week, the current month, the current quarter, and the current year.
- Contributing Risks Trend: This report displays the trend of risks directly associated with business applications and how they are performing over a period. Other downstream risks that contribute to the application risk rating are not represented in this report.

## Audit Overview

The Audit Overview tab appears when you activate the Audit plugin. The Audit Overview tab provides an overview of audit and audit activities related to business applications and displays the following reports:

- Open Audit Engagements: This report displays the number of audit engagements in open state.
- Ineffective Controls: This report displays the number of ineffective controls for an audit engagement.
- Open Issues: This report displays the number of open issues for an audit engagement.
- Past Due Issues: This report displays the number of past due audit issues for an application.
- Upcoming Audit Engagements: This report displays the monthly count for the upcoming audit engagements.
- Open Issues by Audit Engagements: This report displays the monthly count for the open audit issues.
- Past Due Issues by Audit Engagements: This report displays the past due audit issues over a period.
- Ineffective Controls by Audit Engagements: This report displays the information regarding audit engagements and the associated ineffective controls.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

The following filters can be used to filter data on the reports:

- Business Application
- Audit Engagement
- Criticality

## Policy Exceptions Overview

The Policy Exceptions Overview tab appears when you activate the Policy and Compliance plugin. The Policy Exception Overview tab provides information about policy exceptions requested for business applications. The data displayed in the Policy Exceptions Overview tab can be filtered using the Business Application filter. This tab displays the following reports:

- New Exceptions: This report provides information about the new exceptions requested.
- Approved Exceptions: This report provides information about the number of approved exceptions.
- Rejected Exceptions: This report provides information about the number of rejected exceptions.
- Expired Exceptions: This report provides information about the number of expired exceptions.
- Exceptions Awaiting Approval: This report provides information about the exceptions that are awaiting approval and are due on the current date, the current week, the current month, and the current quarter.
- Extensions Awaiting Approval: This report provides information about the extensions that are awaiting approval and are due on the current date, the current week, the current month, and the current quarter
- Upcoming Exceptions Expirations: This report provides information about the exceptions that are about to expire and which are due on the current date, the day after the current date, the current week, the week after the current week, and the current month.
- Exceptions Requested vs. Approved: This report provides information about the exceptions requested versus the number of exceptions approved per month.

## Issues Overview

The Issues Overview tab appears when you activate either the Risk Management plugin or the Policy and Compliance Management plugin. The Issues Overview tab provides information about the various compliance and risk issues associated with business applications. The data displayed in the Issues Overview tab can be filtered using the Business Application filter. This tab displays the following reports:

- Open Issues: This report displays the number of issues in open state.
- Critical Priority Issues: This report displays the number of critical priority issues.
- High Priority Issues: This report displays the number of high priority issues.
- Accepted Issues: This report displays the number of issues that are accepted.
- Past Due Issues: This report displays the number of past due issues.
- Issues to be Resolved: This report displays the number of issues that must be resolved on the current date, the current week, current month, current quarter, and current year.
- Remediation Tasks to be Completed: This report displays the number of remediation tasks that must be completed on the current date, the current week, current month, current quarter, and current year.
- Past Due Issues: This report displays the number of past due issues over a time period.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

- Past Due Remediation Tasks: This report displays the number of past due remediation tasks over a time period.
- Issue Creation Trend: This report displays the trend of how issues are created over a time period.
- Issue Closure Trend: This report displays the trend of how issues are closed over a time period.
- Remediation Task Creation Trend: This report displays the trend of how remediation tasks are created over a period.
- Remediation Task Closure Trend: This report displays the trend of how remediation tasks are closed over a period.

© 2024 ServiceNow, Inc. All rights reserved.
ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc., in the United States and/or other countries.
Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.