



Washington DC Better Together

Last updated: 02/01/2024

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

Table of Contents

Solutions..... 4

 Improve visibility into organizational risk exposure with advanced project risk assessment..... 4

 Automating and optimizing your services and operations using Service Operations Workspace..... 6

 Track the performance of your IT assets using Hardware Asset Management and Sustainable IT..... 10

 Minimize risk by assessing suppliers during the onboarding process..... 12

Solutions

With Solutions, enhance the functionality of ServiceNow applications by using them in combination with each other.

Available Solutions

Learn more about the benefits of each solution and how to implement and use them.

Improve visibility into organizational risk exposure with advanced project risk assessment

With advanced risk assessment for your projects, you can easily identify if any projects pose potential organizational risks and quickly decide on mitigating actions. Combine project risk management with enterprise risk management and get better visibility into your organization's overall risk exposure.

Combined benefits of integrating Project Portfolio Management with Advanced Risk

Feature	Project Portfolio Management	Advanced Risk	Both applications together
Project risk assessment	✓	✗	✓
Elevating to enterprise risk	✗	✗	✓
Assessing inherent and residual risks	✓	✓	✓
Integrated project and enterprise risk registers	✗	✗	✓
Risk heatmaps	✗	✓	✓
Enterprise project risk overview dashboard	✗	✗	✓

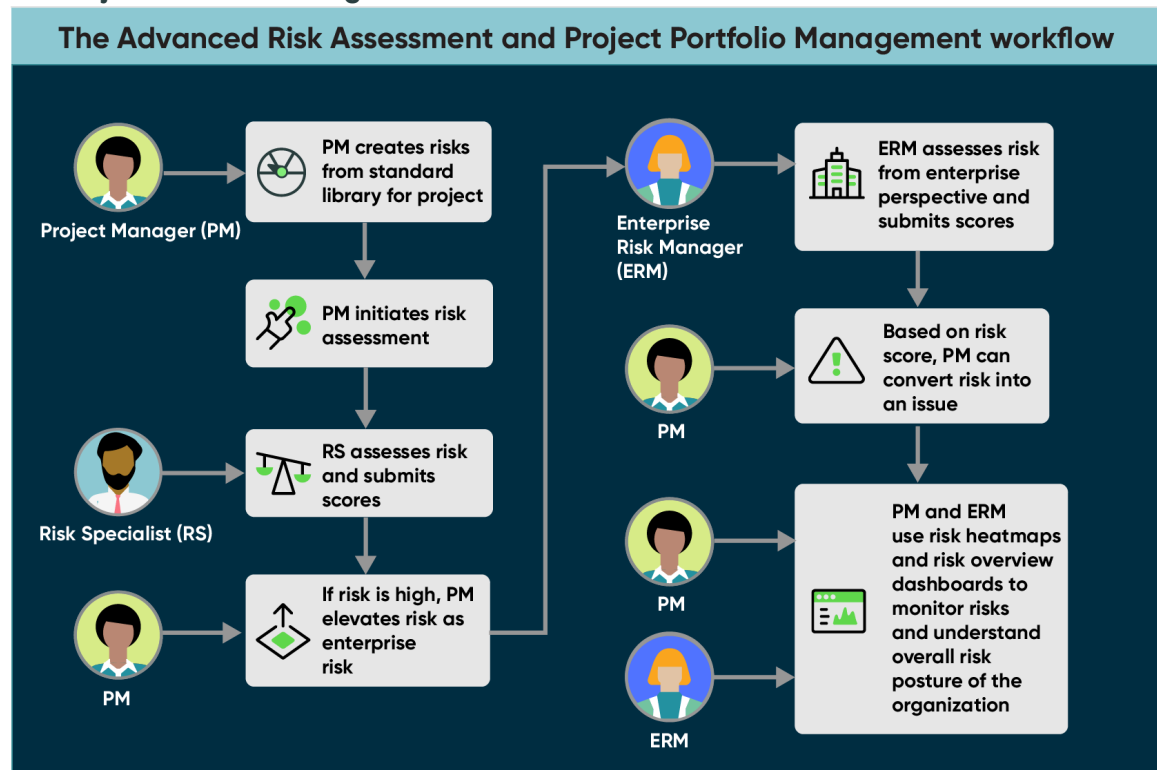
Workflow of advanced project risk assessment

Use Project Portfolio Management (PPM) and Advanced Risk Assessment (ARA) together for these benefits:

- Monitor your risk exposure at the organization level
- Integrate your risk management system for both project and enterprise risk teams.

The following figure shows an example workflow of how a project manager, risk specialist, and enterprise risk manager use the applications together to assess and mitigate risks both at the project and enterprise level.

The Project Portfolio Management and Advanced Risk workflow



In this workflow:

1. The project manager creates risks from the standard library for the project and then initiates the risk assessment.
2. The risk specialist assesses the risk and gives it an assessment score.
3. If the risk score is high, the project manager elevates the risk as an enterprise risk.
4. The enterprise risk manager assesses the risk from the enterprise perspective and gives it an assessment score.
5. Based on the risk score, the project manager can convert the risk into an issue.
6. The project manager and enterprise risk manager use risk heatmaps and risk overview dashboards to monitor risks and understand the overall risk posture of the organization.

Requirements for Project Portfolio Management and Advanced Risk integration

1. Activate the Project Portfolio Management plugin [com.snc.financial_planning_pmo].
2. Install the GRC: Advanced Risk application from the ServiceNow® Store.

Get started with advanced project risk assessment

To get started with assessing your project risks, follow these steps:

1. Setup and configure the risk assessment methodology. See [Configure Project Portfolio Management and Advanced Risk integration](#) .

Role: sn_risk.admin.

2. Define scope and initiate risk assessment. See [Add risks for a project](#).

Role: it_project_manager.

3. Perform risk assessment. See [Perform risk assessment](#).

Role: sn_grc.business_user.

4. Assess and elevate to project risk. See [Elevate a project risk to enterprise risk](#).

Role: it_project_manager.

5. Convert risk to issue and monitor security posture. See [Monitor risk posture](#).

Role: sn_risk.admin, it_project_manager.

Automating and optimizing your services and operations using Service Operations Workspace

You can expand services while reducing costs, delivering high-quality customer and employee experiences, and driving operational resilience. Use a single cloud platform that integrates IT processes such as incident, problem, and change with IT operations such as discovery, business service definitions, service mapping, and event management.

Combined benefits of integrating Service Operations Workspace for IT Service Management (ITSM) and IT Operations Management (ITOM)

Benefits with Service Operations Workspace for ITSM and ITOM



Provides a unified experience for services and operations



Eliminates silos by connecting services and operations teams



Creates and extends processes using low-code configuration



Increases productivity and keeps employees engaged



Optimizes processes for faster resolution of outages and incidents

Feature	Service Operations Workspace for ITSM	Service Operations Workspace for ITOM	All applications together
Simple, intuitive, and clear user interface (UI)	✓	✓	✓
Automated recommendations based on user actions	✓	✓	✓
Tailored landing page providing an overview of tasks	✓	✓	✓

Feature	Service Operations Workspace for ITSM	Service Operations Workspace for ITOM	All applications together
Effective incident management for service desk agents	✓	✗	✓
Experts on call for high-priority tasks	✓	✗	✓
Onboarding experience for logged-in users	✓	✓	✓
Walk-up experience	✓	✗	✓
Request management from incidents and interactions	✓	✗	✓
Guided experience for initial configuration of Service Operations Workspace	✓	✗	✓
Presentation of a service's complete context with related metrics, logs, and additional information	✗	✓	✓
Quick remediation for alerts of a service	✗	✓	✓
Quick automation for operators when using an embedded playbook experience within the alert forms	✗	✓	✓

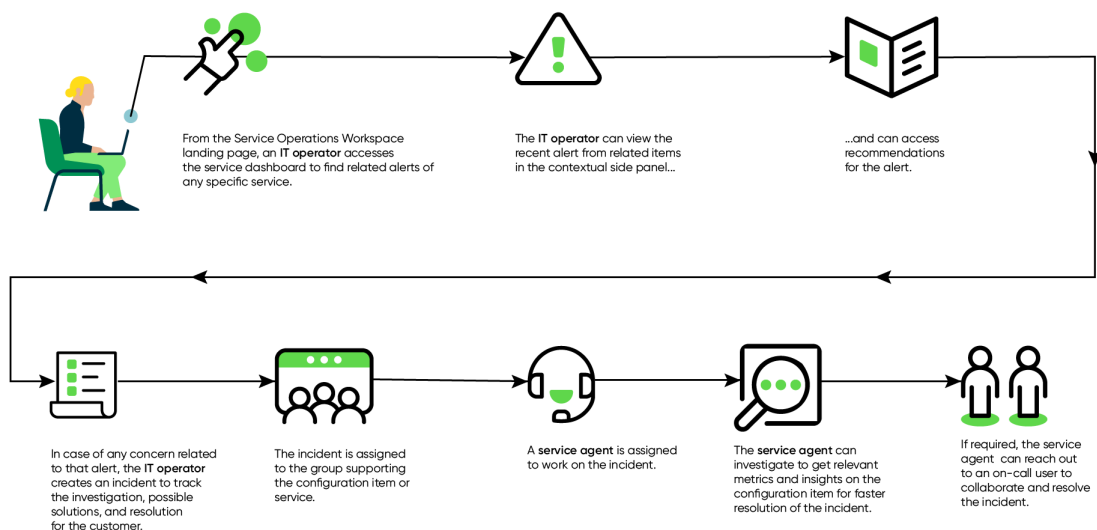
Workflow for Service Operations Workspace

Use Service Operations Workspace for IT Service Management (ITSM) and IT Operations Management (ITOM) together for these benefits:

- Provide a unified experience for services and operations on a single platform.
- Eliminate silos by connecting services and operations teams.
- Increase productivity and keep employees engaged.
- Create and extend ITSM and ITOM processes with low-code configuration.
- Optimize ITSM and ITOM processes for faster resolution of incidents and outages.

The following figure shows an example workflow of how an IT operator and a service agent (service desk agent or L2/L3 specialist) can use these applications to resolve a customer issue.



Service Operations Workspace for ITSM and ITOM workflow



In this workflow:


1. From the Service Operations Workspace landing page, an IT operator accesses the service dashboard to find related alerts of any specific service.
2. The IT operator can view the recent alert from related items in the contextual side panel.
3. The IT operator can access recommendations for the alert.
4. If there is any customer issue related to that alert, the IT operator creates an incident to track the investigation, possible solutions, and resolution for the customer.
5. The incident is assigned to the group supporting the configuration item or service.
6. A service agent such as a service desk agent or L2/L3 specialist is assigned to work on the incident.
7. The service agent can investigate to get relevant metrics and insights on the configuration item for faster resolution of the incident.
8. If required, the service agent can reach out to an on-call user to collaborate and resolve the incident.


Requirements for integrating Service Operations Workspace for ITSM and ITOM


1. Ensure that the following conditions are met for Service Operations Workspace for ITSM.
 - a. Procure the ITSM Standard license or later for ServiceNow® IT Service Management applications. Contact your ServiceNow account manager or sales representative.
 - b. If you want to use Investigation Framework within Service Operations Workspace for ITSM, procure the ITSM Professional license or later for ServiceNow® IT Service Management applications.
 - c. Install Service Operations Workspace ITSM Applications from the ServiceNow® Store. For information about installing this application, see [Install Service Operations Workspace ITSM Applications](#) .
2. Ensure that the following conditions are met for Service Operations Workspace for ITOM.
 - a. Procure the ITOM Professional license or later for ServiceNow® IT Operations Management applications. Contact your ServiceNow account manager or sales representative.
 - b. Install Service Operations Workspace ITOM Applications from the ServiceNow® Store. For information about installing this application, see [Install Service Operations Workspace for ITOM Applications](#) .


Get started with Service Operations Workspace for ITSM and ITOM


To get started with Service Operations Workspace for ITSM and ITOM, follow these steps:


1. Configure Service Operations Workspace for ITSM.
 - a. Set up Service Operations Workspace for ITSM. See [Setting up Service Operations Workspace for ITSM](#) .

Role: admin.
 - b. Set up Investigation Framework. See [Setting up Investigation Framework in Service Operations Workspace](#) .

Role: admin.
 - c. Configure Recommendation Framework for an incident. See [Configuring Recommendation Framework in Service Operations Workspace for ITSM](#) .

Role: admin.
2. Configure Service Operations Workspace for ITOM.
 - a. Set up Service Operations Workspace for ITOM. See [Setting up Service Operations Workspace for ITOM](#) .

Role: evt_mgmt_operator.
 - b. Configure alert metrics. See [Configure alert metrics](#) .

Role: evt_mgmt_operator.
 - c. Configure the Recommendation Framework for an alert. See [Configuring Recommendation Framework in Service Operations Workspace for ITOM](#) .

Role: evt_mgmt_admin.

- d. Configure the Service Operations Workspace inbox. See [Configure the inbox in Service Operations Workspace for ITOM](#).

Role: evt_mgmt_admin.

- e. Customize Service Operations Workspace lists. See [Customize lists in Service Operations Workspace for ITOM](#).

Role: itil.

Track the performance of your IT assets using Hardware Asset Management and Sustainable IT

The Sustainable IT application enables you to effectively manage and monitor the emissions generated by your hardware assets. Additionally, it enables you to keep track of the energy consumption of your assets and their proper disposal after they reach the end of their lifespan.

Combined benefits of integrating Hardware Asset Management and ESG Management's Sustainable IT

Feature	Hardware Asset Management	ESG Management	All applications together
Hardware asset Inventory Management	✓	✗	✓
Estimate hardware asset energy consumption and emissions	✗	✓	✓
Hardware asset Lifecycle Tracking	✓	✗	✓
Report reduction in e-Waste	✗	✓	✓
Increase the proportion of Energy Star-certified assets within the portfolio	✗	✗	✓
Track data center energy consumption, carbon, and renewables	✗	✓	✓
Monitor PUE, WUE and CUE from each location for targeted improvement	✗	✗	✓
Track all relevant Sustainable IT metrics at a glance	✗	✗	✓

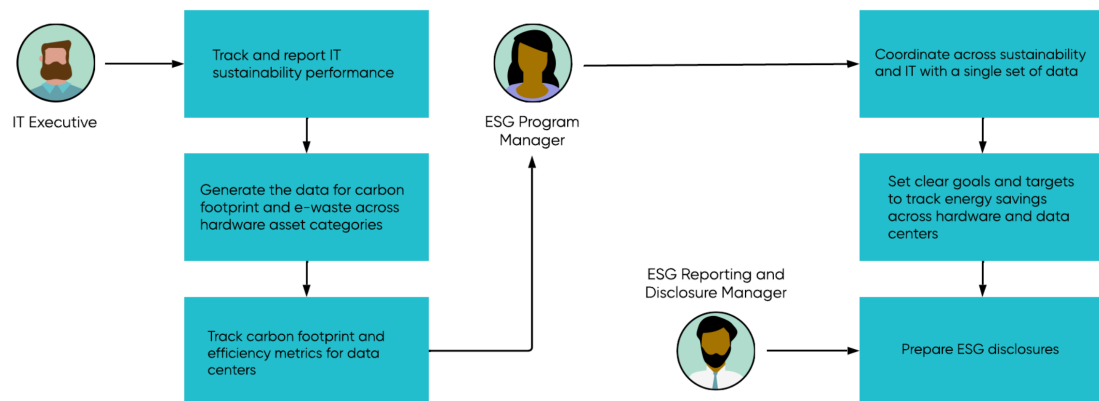
Workflow for using Hardware Asset Management and Sustainable IT

Using Hardware Asset Management and Sustainable IT applications together provides the following benefits:

- Enables you to effectively manage and monitor the emissions generated by your hardware assets
- Helps you to keep track of the energy consumption of your assets and their proper disposal after they reach the end of their lifespan.
- Provides valuable insights through a dashboard, enabling you to make informed decisions on whether to retire or repurpose these assets

The figure illustrates the collaborative efforts between an IT executive and the Sustainability program manager in collecting data on carbon footprint and e-waste. The ESG program managers establish goals and targets to monitor the efficacy of energy-saving measures and prepare disclosures.

The Hardware Asset Management and Sustainable IT workflow



In this workflow:

1. The IT executive logs in to the Asset Executive Workspace to track and report the IT sustainability performance.
2. The IT executive then gets the carbon footprint and e-waste generated across different hardware asset categories and tracks the carbon footprint and efficiency metrics for data centers.
3. The ESG program manager coordinates between Sustainability and IT with a single shared set of data.
4. The ESG program managers establish goals and targets to monitor the efficacy of energy-saving measures and thus help the ESG reporting and disclosure manager to prepare disclosures.
5. The ESG reporting and disclosure manager prepares the ESG disclosures.

Requirements for integrating Hardware Asset Management and ESG Management

1. Install and activate the Sustainable IT (sn_esg_sustain) plugin.
2. Install and activate the Hardware Asset Management (sn_hamp) plugin.

Get started with using Sustainable IT to track your emissions data from your IT assets

Get started with Sustainable IT by completing these tasks:

1. [Activate the Sustainable IT plugin](#).
2. [Filter and activate the Sustainable IT metric definitions](#).
3. [Create new entities for data centers](#).
4. [Manually set up entities for Sustainable IT data centers](#).
5. [Configure Sustainable IT](#).

Minimize risk by assessing suppliers during the onboarding process

With Risk Assessments Integration for Supplier Lifecycle Operations, you can identify and assess potential supplier risks when onboarding new suppliers.

Combined benefits of integrating Supplier Lifecycle Operations with Third-party Risk Management

Feature	Supplier Lifecycle Operations	Third-party Risk Management	All applications together
Supplier onboarding	✓	✗	✓
Information and data management	✓	✗	✓
Case and dispute management	✓	✗	✓
Risk onboarding	✗	✓	✓
Third-party risk due diligence, external and internal risk assessment	✗	✓	✓
Risk intelligence	✗	✓	✓
Risk scoring and monitoring	✗	✓	✓
Risk executive dashboard	✗	✓	✓

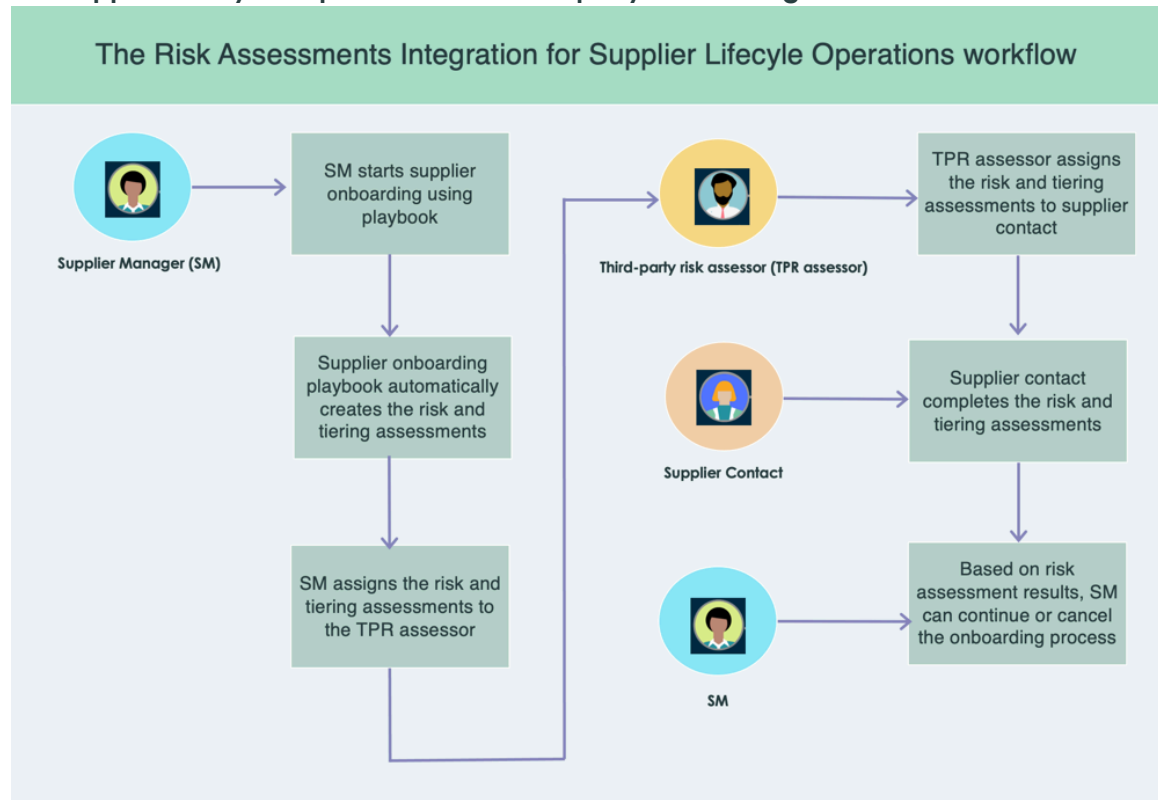
Workflow of Risk Assessments Integration for Supplier Lifecycle Operations

Use Supplier Lifecycle Operations and Third-party Risk Management together for these benefits:

- Evaluate supplier risk when onboarding suppliers
- Analyze risk score to determine whether to onboard a supplier

The following figure shows an example workflow of how a supplier manager and a third-party risk (TPR) assessor can use the applications together to evaluate supplier risk.

The Supplier Lifecycle Operations and Third-party Risk Management workflow



Note: In the Vancouver release, the Vendor Risk Management (VRM) application has been renamed to Third-party Risk Management (TPRM). The VRM application isn't licensed anymore. However, the existing users who have installed VRM can continue to use this workflow to integrate Supplier Lifecycle Operations with VRM for conducting supplier risk and tiering assessments.

In this workflow:

1. The supplier manager receives a supplier onboarding request.
2. The supplier manager uses the onboarding playbook, which provides a streamlined and guided process to onboard suppliers. For more information, see [Using the supplier onboarding playbook to onboard suppliers](#).
3. During the onboarding process, the playbook automatically creates the risk and tiering assessments.

Performing a risk assessment is a key aspect of onboarding a supplier. The supplier risk assessment is done by the third-party risk (TPR) assessor. For more information, see [Get started with Risk Assessments Integration for Supplier Lifecycle Operations](#).

4. The supplier manager assigns the risk and tiering assessments to the third-party risk assessor.
5. The TPR assessor sends the assessments to the supplier's primary contact.
6. The supplier contact logs in to the Supplier Collaboration Portal and completes the risk and tiering assessment.
7. After the risk assessment has been completed, the supplier manager can use the risk information in combination with any other data and determine whether to continue or cancel the onboarding process.

8. After the supplier manager completes the different activities in each stage of the playbook, the supplier is successfully onboarded.

Requirements for integrating Supplier Lifecycle Operations and Third-party Risk Management

1. Install the Supplier Lifecycle Operations application from the ServiceNow® Store. For more information, see [Install Supplier Lifecycle Operations](#).
2. Install the Third-party Risk Management application from the ServiceNow® Store. For more information, see [Configuring Third-party Risk Management](#).

Get started with Risk Assessments Integration for Supplier Lifecycle Operations

Get started with Risk Assessments Integration for Supplier Lifecycle Operations by completing these tasks:

1. Create a supplier. For more information, see [Create a supplier from the Source-to-Pay Workspace](#).
2. Onboard a new supplier using playbooks. For more information, see [Using the supplier onboarding playbook to onboard suppliers](#).

Depending on whether you've installed Third-party Risk Management, the playbook does the following:

- If you have installed Third-party Risk Management, the playbook creates the risk and tiering assessment records. The risk and tiering assessment records are also listed in the **Risk Assessments** and **Tiering Assessments** tabs, respectively. The supplier owner or supplier manager assigns these records to the TPR assessor.

Onboard new supplier: Supplier

Supplier Assigned to Requested by State Priority Due date
Supplier Deanna Gerbi Deanna Gerbi Awaiting task com... 3 - Moderate 2023-10-04 08:00...

Playbook Details Supplier Tasks Related Cases Approvals Draft Emails **Risk Assessments** Tiering Assessments Documents

Supplier onboarding

- Registration Complete
 - Show possible duplicate suppliers
 - Show possible duplicate onboarding requests
 - Check for supplier intelligence source
 - Import supplier details from intelligence/external source
 - Verify that the supplier information is correct
- Qualification 3 remaining 2
 - Check if Vendor Risk Management is installed
 - Show Risk Assessment record**
 - Show Tier Assessment record

Show Risk Assessment record

In Progress List

M Assigned to Me

Show a record list, so supplier managers can navigate to the newly created assessment.

Risk assessment for Supplier

Name State

Risk assessment for Supplier Draft

Mark Complete Open List Skip

- If you've not installed Third-party Risk Management, the playbook creates supplier cases of types **Risk assessment** and **Tiering assessment**. The Supplier Risk Assessment and Supplier Tiering Assessment cases are child cases of the parent **Onboard a Supplier** case

and are displayed on the **Related Cases** tab. The supplier owner or supplier manager assigns these assessment cases to the TPR assessor.

Onboard new supplier: Supplier

Supplier	Assigned to	Requested by	State	Priority	Due date
Supplier	Deanna Gerbi	Deanna Gerbi	Awaiting task com...	3 - Moderate	2023-10-04 08:00...

[Playbook](#)
[Details](#)
[Supplier Tasks](#)
[Related Cases](#)
[Approvals](#)
[Draft Emails](#)
[Risk Assessments](#)
[Tiering Assessments](#)
[Documents](#)

- As a supplier contact, you can log in to the Supplier Collaboration Portal and complete the risk and tiering assessments. For more information, see [Complete a risk assessment from the Supplier Collaboration Portal](#).
- As a supplier manager, you can use the assessment result data in combination with any other data to determine whether to continue or cancel the onboarding process.