



Brazil Better Together

Last updated: 10/07/2026

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

 Case Study: Enhancing Risk, Compliance, and Audit Management with ITOM..... 10

 Employee Service Management Foundation..... 11

 Building desktop automations from Task Mining data..... 12

 Requirements and limitations..... 15

 Create an automation request in Task Mining..... 16

 Create automation blocks from the automation request in Automation Center..... 18

 Create an AI agent and desktop actions from Automation Center..... 21

 Example: Execute employee onboarding automatically..... 24

 Track the performance of your IT assets using Hardware Asset Management and Sustainable IT..... 28

 Minimize risk by assessing suppliers during the onboarding process..... 30

 Enhancing the asset procurement experience using IT Asset Management (ITAM) and Sourcing and Procurement Operations (SPO)..... 34

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	✗	✗	✓

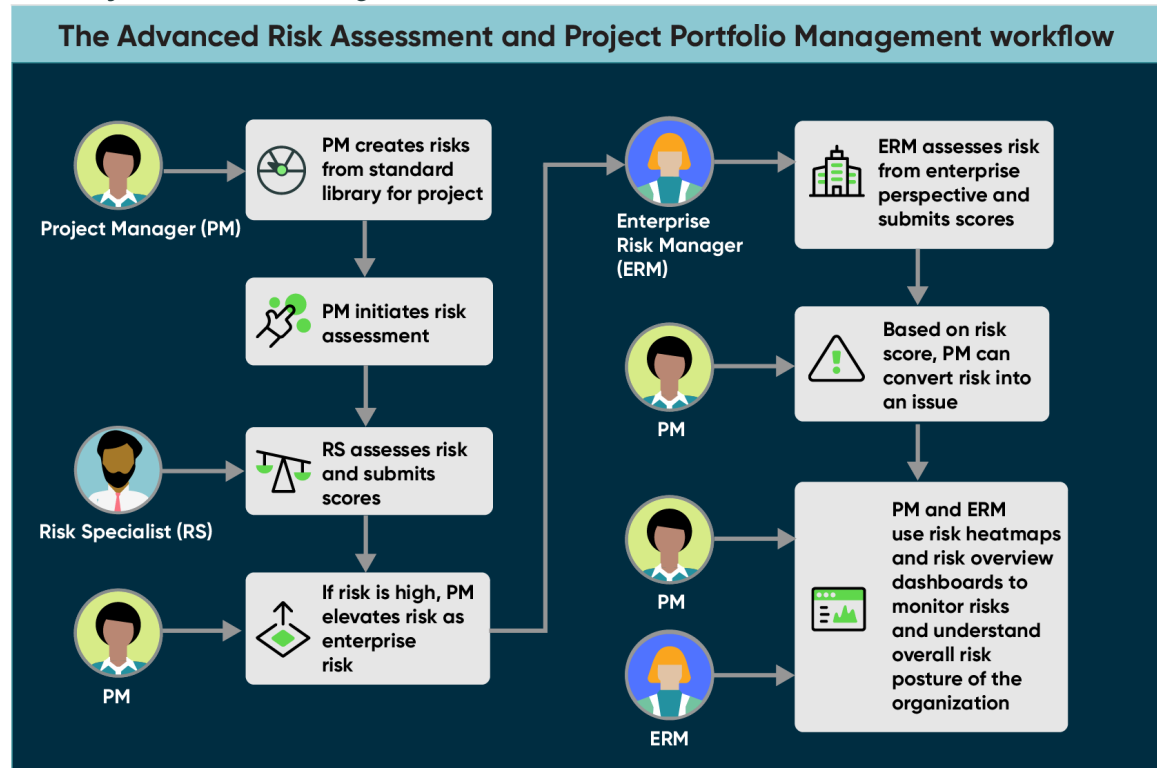
Workflow of advanced project risk assessment

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	✗	✓	✓

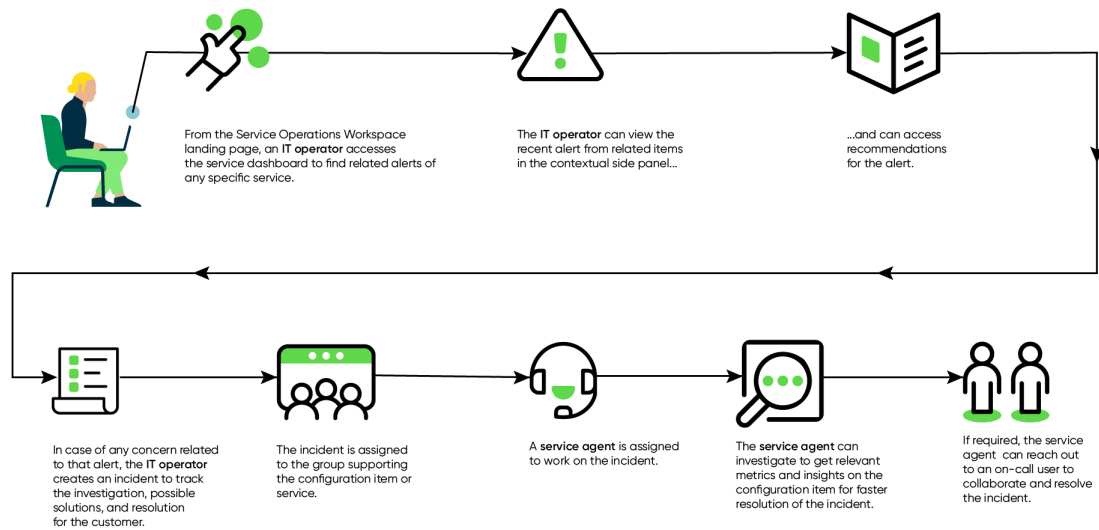
Workflow for Service Operations Workspace

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](#) .
 - 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](#) .
 - 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.

Case Study: Enhancing Risk, Compliance, and Audit Management with ITOM

The use case demonstrates how ITOM integration streamlined risk, compliance, and audit management for a financial institution by providing real-time operational visibility, automation, and enhanced risk assessments.

Problem Statement

A leading financial institution sought to streamline its risk management processes as it grew, handling increasingly complex operational, third-party, and technology risks, along with compliance and internal audit functions. The institution recognized the need for a unified platform to improve efficiency and reduce manual effort.

Challenges

- **Lack of centralized visibility:** The financial institution faced challenges in maintaining a clear, real-time view of risks, compliance, and audit processes. Disparate systems made it difficult to assess operational risks linked to IT services and infrastructure.
- **Siloed IT infrastructure:** The disconnected IT systems of the institution made it challenging to monitor and respond to operational issues that could affect risk management functions, such as downtimes, configuration errors, and IT service failures.
- **Limited use of existing data:** The significant amount of IT data available from various sources wasn't fully utilized for risk and compliance management due to the lack of integration with existing systems.

ITOM-specific solutions

- **Real-time operational visibility:** ITOM provided the institution with real-time insights into the health, availability, and performance of IT services. By integrating ITOM with ServiceNow IRM, risk and compliance teams were able to correlate operational risks (e.g., service outages, performance degradation) directly with broader risk management efforts.
- **Automated Service Mapping for better risk assessment:** The Service Mapping capabilities in ITOM enabled the institution to automatically map IT services and understand their dependencies. This was critical for assessing operational risks in real time. For example, the system could detect a critical service failure and immediately flag it as a high-risk event in the compliance dashboard, allowing the institution to take pre-emptive action.
- **Proactive monitoring and alert response:** By leveraging ITOM Event Management, the institution was able to monitor key operational risks, such as system failures and third-party service outages, and trigger automated alerts to relevant risk management and compliance teams. This proactive approach minimized the time between identifying an operational risk and responding to it.

- **Configuration Management Database (CMDB) for Compliance:** The integration of ITOM with the CMDB ensured that all IT assets, configurations, and their relationships were accurately tracked. This provided a single source of truth for risk management, enabling compliance teams to automatically link risks to specific IT assets or services, ensuring more precise risk assessments, especially in the context of technology risks and third-party dependencies.
- **Alert noise reduction and automation:** ITOM AIOps was leveraged to reduce alert fatigue by automatically grouping and correlating related alerts (such as from infrastructure failures). This reduced manual effort for risk and compliance teams to sift through irrelevant alerts, allowing them to focus on higher-priority operational risks.

Key outcomes

- **Unified Risk and IT operations:** By integrating ITOM with ServiceNow IRM, the institution achieved a unified view of both operational and IT risks. This integration facilitated the identification of risks stemming from operational IT failures, helping the institution quickly address critical alerts before they escalated.
- **Improved efficiency through automation:** ITOM automation helped the institution eliminate manual processes related to operational risk monitoring, such as manually tracking service disruptions or changes in the IT environment that could introduce new risks.
- **Enhanced compliance with IT-Related regulations:** The real-time data provided by ITOM ensured that the institution could meet regulatory requirements around IT risks and audit readiness. The ability of ITOM to keep all IT assets and configurations up to date made audit processes faster and more accurate.
- **Scalability for future risk management needs:** The cloud-native architecture of ITOM provided scalability and flexibility, ensuring that the institution could continue to manage risks as it grew. ITOM also supported mobile access, enabling remote monitoring and alert management by risk and IT teams.

Employee Service Management Foundation

Employee Service Management Foundation unifies IT, HR, finance, legal, and workplace services on a single platform. This integrated approach streamlines service delivery and reduces administrative overhead for growing organizations.

Combined benefits of integrating Core Business Suite with ITSM Foundation

Feature			All applications together
	✓	✗	✓
	✗	✓	✓

Workflow for ESM Foundation

Using Core Business Suite with ITSM Foundation together provides the following benefits:

-
-

The Core Business Suite with ITSM Foundation workflow

In this workflow:

- 1.
- 2.

Requirements for integrating Core Business Suite with ITSM Foundation

- 1.
- 2.
- 3.

Get started with

Get started with by completing these tasks:

- 1.
- 2.
- 3.

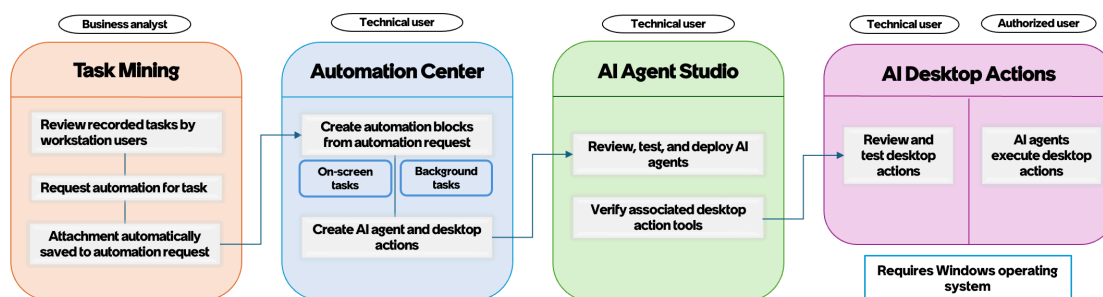
Building desktop automations from Task Mining data

Automatically convert desktop processes into executable AI agents: capture the task (desktop processes) in Task Mining, create desktop actions (automation blocks) and AI agent in Automation Center, and test and deploy the AI agent in AI Agent Studio.

This feature currently supports only Excel-to-browser interactions, where data is copied from a Microsoft Excel file and it is entered into a form in a browser.

Note: This feature uses generative AI to produce automation. AI-generated content, including automation blocks and agent instructions, may be inaccurate or incomplete. Review and validate AI-generated output before activating an agent.

Automation workflow stages



Stage 1: Capture and refine (Task Mining)

- Workstation users use the Task Mining agent to capture their desktop processes end-to-end, including interactions across multiple applications for the selected project. Agent captures screenshots and UI interaction metadata of steps users perform.

- Business analyst runs a mining job on the project to generate an analysis of the collected data (desktop activities).
- Captured desktop activities are stored as tasks in Task Mining.

Stage 2: Automate (Task Mining + Automation Center)

- Business analysts review the task timeline to define specific optimization opportunities and automation candidates, and submit an automation request for the task in Task Mining.
- Automation Center captures the structured data in an automation request for AI-powered step generation and automation block creation.
- Technical users generate automation blocks (on-screen and background tasks) from the automation request in Automation Center.
- Based on the automation request, an AI agent and desktop actions are created in Automation Center.

Stage 3: Deploy (AI Agent Studio)

- Technical users with the sn_aia.admin role verify auto-generated agent name and description, agent steps, and desktop action tools in AI Agent Studio.
- Technical users test and deploy the AI agent in AI Agent Studio.

Stage 4: Execute (AI Desktop Actions)

- Authorized users invoke deployed AI agents from the ServiceNow Otto panel, where the agent automatically executes the complete desktop automation process.
- The agent runs both background tasks (such as fetching data from source files) and on-screen tasks (such as navigating web applications and entering form data) desktop actions in AI Desktop Actions on the Windows machine, completing the entire workflow without user intervention.

Example: Employee onboarding automation

A human resources team needs to automate the employee onboarding process. Each new hire currently requires:

1. Reading new hire data from an Excel spreadsheet (background task) for creating an employee record in the HR system
2. Entering employee information into a web form (on-screen task)
3. Provisioning an email account in Microsoft 365 (on-screen task)
4. Adding the new hire to the team distribution list in Microsoft Outlook (on-screen task)

This multi-application workflow is ideal for desktop automation. The team uses Task Mining to capture the actual onboarding steps performed by HR staff. Then, the technical user converts those steps into an automated agent that can execute the entire workflow end-to-end.

Progressive refinement

The workflow supports progressive refinement at each stage:

1. Validate Task Mining captured the right interactions.
2. Verify Automation Center extracted meaningful workflow components.
3. Validate on-screen task desktop actions on the AI Desktop Actions design workspace.
4. Verify the description and instructions of the AI agent and test it in AI Agent Studio.
5. Execute the complete workflow end-to-end in AI Desktop Actions execution workspace.

This staged approach reduces risk and enables early detection of issues before deploying full automations.

Persona and roles

The automation creation journey involves four key personas:

Persona and roles

Persona	Responsibilities	Key skill
Business analyst	Reviews tasks, edits captured steps, and creates Automation Request records in Task Mining.	Process documentation, data validation
Technical user	<p>Creates production-ready desktop actions and AI agents from the automation request in Task Mining.</p> <p>Reviews and approves desktop actions. Deploys agents to target instances and performs end-to-end testing in AI Agent Studio.</p> <p>Note: The <code>sn_aia.admin</code> role is required for editing and testing the AI agent.</p>	Automation development, testing, deployment
Authorized user	<p>Business users, process owners, or operations team members with no automation development experience execute desktop actions in the Windows environment.</p> <p>Note: The <code>now_assist_panel_user</code> role is required for executing the desktop actions in AI Desktop Actions.</p>	Executing desktop actions

Key benefits

Automated process documentation

By building automation skeletons directly from Task Mining data, ServiceNow eliminates the need to manually construct baseline automation logic.

Reduced clarification cycles

Automation artifacts include desktop actions, task steps, input/output mappings, and guardrails.

Developers receive a pre-configured structure that already contains:

- Identified steps in the correct sequence
- Relevant data mappings

- UI element references
- Initial tool connections

Self-service desktop action review

Developers can open and validate desktop actions on their own Windows machine, ensuring captured intent matches actual process steps.

AI agent pre-population

AI Agent Studio is automatically populated with agent name, specialty description, tools, and tool descriptions sourced directly from the task breakdown.

Reduction in authoring time

This approach saves development time compared to building agents from scratch without predefined tool connections and configurations.

What to explore next

- [Requirements and limitations](#)
- [Create an automation request in Task Mining](#)
- [Create automation blocks from the automation request in Automation Center](#)
- [Create an AI agent and desktop actions from Automation Center](#)

Related topics

[Create Task Mining project](#) 

[Create a Task Mining project](#) 

[Install the Task Mining agent](#) 

[Categorize workstation activities to simplify analysis](#) 

[Task Mining agent](#) 

[Defined desktop actions in AI Desktop Actions](#) 

[Test and activate a desktop action in AI Desktop Actions](#) 

[Create an AI agent](#) 

[Examples of executing desktop actions using AI agents](#) 

Requirements and limitations

Learn about requirements and limitations for this unified journey.

Requirements

- Application dependencies: Task Mining, Automation Center, AI Agent Studio, and AI Desktop Actions.
- Windows requirement: Task Mining agent recording and AI Desktop Actions agent execution require Windows 11+. Automation Center configuration and agent creation can be performed on any supported operating system.
- Instance requirements: starting with the Brazil patch 4 release.

- **Plugin dependencies:** Both Automation Center and AI Desktop Actions must be installed on the target instance before you can create an AI agent. ServiceNow Otto for Automation Center must be installed to use this feature.
- **AI skill dependencies:** User task step summarization skill must be activated. For more information, see [Activate a skill](#).

Limitations

- **Supported scenario:** This feature currently supports only Excel-to-browser interactions, where data is copied from a Microsoft Excel file and it is entered into a form in a browser.
- **AI-generated output variability:** Decomposed automations and agent instructions are generated by AI. Each run may produce different results. Review all AI-generated output before creating or activating an agent.
- **Anchor adjustment:** On-screen task desktop actions require anchors that identify the UI element to interact with. Anchors captured from Task Mining recordings may not match the format AI Desktop Actions expects and may require manual correction in the AI Desktop Actions design workspace.
- **No cross-product notification:** Automation Center users don't receive a notification when a Task Mining user submits an automation request. The business analyst and the technical user must coordinate directly.

Related topics

[Data collected by Task Mining](#)

[Task Mining agent](#)

Create an automation request in Task Mining

As a business analyst, review the task timeline for identifying task optimization opportunities and automation candidates. Then, submit an automation request from Task Mining to create an automation in Automation Center.

Before you begin

- [Create a Task Mining project](#) in Task Mining.
- Confirm that you select **Capture screenshots to create desktop actions** option while defining the scope for the task. For more information, see [Define user actions for task logging](#).
- Enable workstation users to capture desktop activity data that includes desktop interactions and sequence of steps using the Task Mining agent.
- Run a mining job on a Task Mining project to generate an analysis of the collected project data. For more information, see [Run a mining job](#).
- Verify that Automation Center is installed to initiate an automation request.
- Verify that ServiceNow Otto for Platform is installed and the User Task Step Summarization skill is activated to use the AI features in the integration.

Role required: sn_tm_core.analyst, sn_tm_core.power_user, sn_tm_core.admin

About this task

Create automation requests for your tasks directly from Task Mining. Capture both steps and automation properties in a single recording session, instead of recording the same process twice. When a Task Mining analyst submits an automation request, the recording is delivered to the automation team with all UI screenshots and application metadata needed to build desktop actions.

Procedure

1. Navigate to **Workspaces > Task Mining Workspace**.
2. Select the project with a task timeline analysis that you want to identify task improvement actions for and select the **Task timeline** tab.
3. Select the task that you want to act on.
4. **Optional:** Create a copy to make any edits and to take task improvement actions.
 - a. Select **Edit** to create a copy that you use for automation without affecting the original.
 - b. Enter a descriptive name in the **Task name** field.
 - c. Select **Duplicate to edit**.
The new task is created with the task name appended with Editable.
5. **Optional:** Edit any of these steps if you want to change task details.
 - a. Select the Duplicate step icon next to the step to make a copy of the step.
The new task step is created. The **Interaction** column of the duplicated step is empty.
 - b. Select the Delete step icon next to the step to remove a step from the task.
 - c. Select the Reorder step icon next to the step to drag the step to a different order.
 - d. Double-click a task field (or use the keyboard shortcut) to edit details, enter the new text, and select **Apply**.
You can't edit the **Source** and **Datetime** fields.
6. From the selected task, select **Request automation**.
7. Select the task improvement action that you want to take, and select **Continue**.

Option	Description
Generate with AI	Open an Automation Center request based on the improvement opportunity. Populate the Description and Detailed sequence of steps fields with data from the tasks. For more information, see step 8.
Complete manually	Fill in the Automation Center request form with details of the improvement opportunity, and submit the request. Note: If an automation request has already been made for this task, a message with a link to the existing automation request is provided.

8. **Optional:** Select **Generate details** to populate the **Description** and **Detailed sequence of steps** fields with data from the tasks again.

(Optional) Review all auto-generated instructions and correct any inaccuracies. The detailed sequence of steps is the basis of the automation.

A maximum of 250 steps can be generated. If your task has more than 250 steps, try selecting a more appropriate task. If you want to continue with the task, you can simplify the steps to reduce their number. Alternatively, you can manually populate the **Description** field with step details and complete the automation request form.

Note: The generate details option is available only if ServiceNow Otto for Platform is installed and the User Task Step Summarization skill is activated.

9. Select **Save**.

An attachment is automatically added to the automation request. The attachment contains the task timeline, screenshots, and interaction summary generated by Task Mining. Automation Center reads this attachment to generate automations. If the attachment is missing, you can request an automation again for the task.

The automation request is created and associated with the task that it was based on. A link to the automation request record is available under the **Automation request** column of the project's Task timeline analysis.

Example: Example: Onboarding automation request

In this example, an HR analyst captures the employee onboarding workflow:

- A workstation user (HR staff member) uses the Task Mining agent to record themselves completing the onboarding process for a new hire
- The agent captures their interactions across the HR system, email interface, and Microsoft Outlook
- The HR analyst reviews the captured task timeline and submits an automation request
- The automation request includes the complete task recording, screenshots, and interaction summary
- Automation Center receives this request and uses it to generate automation blocks

What to do next

In Automation Center, generate automations to create automation blocks from user task patterns captured using *Task Mining*. For more information, see [Create automation blocks from the automation request in Automation Center](#).

Create automation blocks from the automation request in Automation Center

Create automation blocks (on-screen tasks and background tasks) using the automation request created in Task Mining. These automation blocks are used to create desktop actions and AI agent in Automation Center.

Before you begin

- Verify that Automation Center and AI Desktop Actions are installed.
- Verify that ServiceNow Otto for Automation Center plugin is installed and the User task step summarization skill is activated.
- Confirm that the business analyst submitted an automation request in Task Mining. For more information, see [Create an automation request in Task Mining](#).

Role required: sn_aia.admin, sn_ac.automation_admin or sn_ac.automation_technical_user, and sn_tm_core.analyst

About this task

When business analyst submits an automation request from Task Mining, the request appears in Automation Center with the task recording summary saved as an attachment. Use the **Generate automations** option in the Automation tab to break the automation into discrete automation blocks. These automation blocks are used to create an AI agent and desktop actions that are categorized as on-screen tasks and background tasks, which determine how AI agents run them in AI Desktop Actions.

- **On-screen tasks:** Execute automation steps by interacting with the UI. These appear in the AI Agent Studio design workspace, where they can be tested, configured, and validated interactively before agent execution.
- **Background tasks:** Process data based on preconfigured instructions (such as reading information from Excel) without requiring UI interaction. These desktop actions run in background and don't require interactive testing on the design workspace.

Important:

Because automations blocks are created using AI, results may vary between runs. Review all generated automations blocks before you proceed with creating an AI agent and desktop actions.

Procedure

1. Navigate to **Workspaces > Automation center Workspace**.
2. Select the list icon ().
3. On the **Lists** tab, under **Build**, select **All Automation Requests**.
4. Open the automation request submitted by the business analyst.

 **Important:** To find automation requests from Task Mining, check the **Intake source** column on the **All Automation requests** table and look for **Task mining**.

5. Verify that the automation request contains the task recording attachment.

The attachment contains the task timeline and interaction summary generated by Task Mining. Automation Center reads this attachment to generate automations. If the attachment is missing, ask the Task Mining user to resubmit the automation request.

6. Select the Automations tab on the automation request page.
7. Select **Generate automations**.
The **Generate automations** window is displayed.

8. **Optional:** Enter additional instructions in the **Optional context** field to guide the decomposition.

Use additional instructions to focus or constrain the output. For example, you can specify steps to exclude or applications to prioritize. If you skip this step, Automation Center uses only the task recording attachment as an input.

Automation Center reads the task recording attachment and uses AI to create on-screen and background automation blocks from the automation request.

9. Review the generated automations.

Each automation displays the following information:

Automation fields

Field	Description
Name	AI-generated name for the automation.
Execution Mode	Provides information related to the type of automation block created. <ul style="list-style-type: none"> ○ On-screen tasks: For On-screen tasks, screenshots are most important. Without screenshots, these automation blocks aren't generated. ○ Background tasks: For background tasks, instructions are most important.
Description	A summary of the steps the automation performs. This field is used as the basis for the AI Desktop Actions tool instructions and the agent instructions when you create the AI agent. Review this field carefully.

10. Optional: Open each automation to see the details.

Automation fields

Field	Description
Automation name	AI-generated name for the automation.
Target application	The application the automation interacts with, such as Microsoft Excel or a browser.
Input and Output	AI-generated values for the data the automation receives and produces.
Description	A summary of the steps the automation performs. This field is used as the basis for the AI Desktop Actions tool instructions and the agent instructions when you create the agent. Review this field carefully.
Goal and intent	The primary goal of the automation.
Guardrails	Considerations to run the automation smoothly.

11. If the results are unsatisfactory, select **Generate automations** again.

The **Generate automations** window is displayed.

Provide the updates in the **Optional context** field. You can regenerate automations as many times as needed. Each run calls the AI model again and may produce different results, including changes to automations you did not intend to modify. Review all automations after each generation.

i Important: Each prompt starts fresh and doesn't carry forward the previous changes. To keep earlier changes, include all your requirements in one prompt.

Example: Example: Generating onboarding automation blocks

When the HR analyst's automation request arrives in Automation Center, the following automation blocks are created.

Created automation blocks

Task type	Automation blocks
On-screen tasks	<p>Fill HR form</p> <p>Fill HR system form with new hire data.</p> <p>Requires screenshots and UI interaction metadata.</p> <p>Add employee to Outlook</p> <p>Add employee to Outlook distribution list.</p> <p>Requires browser navigation and form interaction.</p>
Background tasks	<p>Read data from Excel</p> <p>Read new hire information from Excel file.</p> <p>Operates silently based on instructions.</p>

The technical user reviews the generated blocks:

- Verifies that the on-screen form-filling task captured all required fields
- Confirms the distribution list task navigates to the correct team list
- Reviews the background task instructions for reading Excel data correctly

What to do next

You can now create an AI agent and desktop actions from the generated automation blocks. For more information, see [Create an AI agent and desktop actions from Automation Center](#).

Create an AI agent and desktop actions from Automation Center

After reviewing the automation blocks generated from an automation request, create an AI agent that executes desktop actions on a Windows machine.

Before you begin

- Verify that Automation Center and AI Desktop Actions are installed.
- Verify that the AI Desktop Actions client application is downloaded and installed on the Windows machine where the AI agent runs.
- Verify that ServiceNow Otto for Automation Center plugin is installed and the User task step summarization skill is activated.

- Confirm that you have created automation blocks from an automation request Automation Center. For more information, see [Create automation blocks from the automation request in Automation Center](#).
- The automation request must be in the **In progress** state.

Role required: sn_aia.admin, sn_tm_core.analyst, sn_ac.automation_admin, sn_ac.automation_technical_user

About this task

When you select **Create agent**, Automation Center converts the generated automation blocks into desktop actions. It also creates a new AI agent pre-populated with instructions, a role description, input parameters, and desktop actions tools. For on-screen tasks, a new desktop action is created using screenshots from the task recording and added as a tool. For background tasks, a tool is created for the background application. If a matching background application is already available, instructions are passed to the existing background application.

After the agent is created, you must review the agent instructions and test each desktop action tool before activating the agent in AI Agent Studio. You must verify and manually adjust the anchors of on-screen desktop actions in AI Desktop Actions.

Important:

Agent testing and AI Desktop Actions tool execution require a Windows machine with the AI Desktop Actions application installed. For more information, see [Download AI Desktop Actions installer for defined desktop actions](#) .

Procedure

1. From the Automation Center workspace, open the automation request.
2. Select the Automations tab on the automation request page.
The Automations tab displays the generated automation blocks. Confirm that you have reviewed and are satisfied with the generated automation blocks before proceeding.
3. Select **Create agent** on the automation request page.

 **Note:** The **Create agent** option is available only if the ServiceNow AI Agents skill is installed and the automation request is in **In progress** state.

The **Choose destination instance** dialog box is displayed.

4. Select an instance to create the agent in, and select **Continue**.
You can select the current instance or any other instance. Verify that the instance you choose has Automation Center and AI Desktop Actions installed.

For information on configuring an instance, see [Create a Connection & Credential alias](#) .

A summary of the agent being created is displayed.

5. Review the agent configuration summary, and select **Create agent in AI Studio**.

An AI agent and desktop actions are created and activated in AI Agent Studio. The desktop actions are automatically added as tools to the AI agent

6. In AI Agent Studio, review the agent instructions.

The agent is pre-populated with the AI-generated content.

Note: AI-generated instructions may not accurately reflect the task. Review and correct the instructions, particularly the input parameter descriptions and the step sequence.

7. In the Define user access step, assign required roles and the `now_assist_panel_user` role to the AI agent so the users with these roles can invoke the AI agent.

Authorized users can invoke the agent from the ServiceNow Otto panel by typing a request that matches the agent's name or description.

Note:

Authorized users don't need access to Automation Center or AI Agent Studio to run the agent. They can invoke it from the ServiceNow Otto panel.

The `now_assist_panel_user` role is required for executing the desktop actions in AI Desktop Actions.

8. In AI Desktop Actions, fix any anchor issues for each on-screen task desktop action.

Important: If there are no on-screen task desktop actions created, then the reason could be that the recording didn't have screenshots. Contact the Task Mining analyst to provide the recording with screenshots.

- a. Open an on-screen task desktop action in the AI Desktop Actions client application.

- b. Test the on-screen task desktop action.

For more information, see [Test and activate a desktop action in AI Desktop Actions](#).

- c. Verify the position of failed anchors and adjust for each screen in the desktop action.

Anchors help identify the UI elements that AI Desktop Actions interacts with, such as the field to select or the button to activate. Anchors generated from Task Mining recordings may not match the format that AI Desktop Actions expects. Common anchor issues include:

- The URL bar is used as an anchor in the Task Mining recording, but AI Desktop Actions can't anchor to the URL bar. Replace URL bar anchors with a specific page element such as a button or field label.
- An anchor targets a UI element that is not reliably present or uniquely identifiable. Select a more stable anchor element.

- d. Repeat testing until each on-screen task desktop action runs without errors on the target application.

Result

AI agent and desktop actions are ready for execution.

Example: Example: Creating the onboarding agent

After reviewing the automation blocks, the technical user selects **Create agent** and:

1. The agent is pre-populated with:

- **Name:** "Employee Onboarding Agent"
- **Description:** "Automates the complete employee onboarding workflow including HR record creation, form entry, and distribution list provisioning"
- **Desktop actions:** Three tools (read Excel, fill HR form, update distribution list)
- **Instructions:** AI-generated steps for executing the onboarding workflow

2. The technical user reviews and adjusts:

- Corrects the input parameter description (specifies that the Excel file location should be provided by the invoking user)
- Verifies the sequence of steps (read data → fill form → update list)
- Assigns the `now_assist_panel_user` role so HR staff can invoke the agent

3. In AI Desktop Actions, the technical user:

- Opens each on-screen task desktop action on their Windows machine
- Tests the form-filling action to verify all fields are populated correctly
- Fixes any anchor issues where the agent may have captured UI element references incorrectly
- Verifies the distribution list update completes successfully

What to do next

When an authorized user types a request in the ServiceNow Otto panel that matches the agent's name or description, the system invokes the AI agent. The AI agent executes the desktop action in the AI Desktop Actions execution workspace on user's Windows machine.

Example: The HR team is now ready to execute the employee onboarding agent. When a new hire is added to the system, an HR coordinator types the new employee's name and hire date into the ServiceNow Otto panel. The AI agent automatically executes the complete onboarding workflow, reducing manual data entry time from 30 minutes to seconds and eliminating errors caused by manual form filling.

For more information about executing desktop actions, see [Examples of executing desktop actions using AI agents](#) .

Example: Execute employee onboarding automatically

As an HR coordinator, automatically onboard new employees by triggering an AI agent that executes the complete employee provisioning workflow from the ServiceNow Otto panel.

Before you begin

To access the AI Desktop Actions functionality, perform the following steps:

- Enable AI Desktop Actions on your ServiceNow instance. For more information, see [Configure AI Desktop Actions](#) .
- Download the AI Desktop Actions installer to automate repetitive tasks across applications and systems. For more information, see [Download AI Desktop Actions installer for defined desktop actions](#) .

Confirm that the following system requirements are met:

- Windows 11 operating system is used.
- A .NET 9.0 runtime v9.0.10 and .NET 9 Desktop Runtime v9.0.10 is installed.

- No extended monitors are connected.
- Theme must match between the systems used for recording and execution.
- Remote Desktop must be enabled on your machine and your account must be granted Remote Desktop access permissions before you start using the AI Desktop Actions Execution workspace.
- Add the end users who interact with the Execution workspace of AI Desktop Actions to the Remote Desktop Users group on the target machine and provide Remote Desktop access permissions for seamless automation execution.

If your organization uses Group Policy, add the end users to a Microsoft Active Directory group that is permitted to use Remote Desktop through Group Policy on each target machine where desktop actions run.

- Local changes to the Remote Desktop Users group are temporary unless they align with Microsoft Active Directory entitlements.
- If the user is not entitled, Group Policy refresh automatically removes them from the group.
- Confirm that your firewall allows bidirectional traffic between the AI Desktop Actions application and your ServiceNow instance on the port 80 for HTTP and port 443 for HTTPS.

If your organization uses non-standard ports for HTTP or HTTPS, confirm the correct ports with your IT administrator before proceeding.

You must have full permissions to create and use system I/O communication pipes.

- If applicable, confirm that the `snada : // custom URI` protocol is registered to launch the AI Desktop Actions application in the browser.
- The employee onboarding AI agent is deployed and active in your instance.
- The HR system (containing the employee form) and Microsoft 365 admin portal are accessible from the Windows machine.
- New hire data is available in the designated Excel spreadsheet with columns for: Employee Name, Employee ID, Department, Manager, and Email Address.
- The service account running the agent has credentials configured for HR system access and Microsoft 365 admin portal access.

Note: Screen resolution and scaling must be the same between the systems used for recording the agent's desktop actions and the execution environment.

Familiarize yourself with the AI Desktop Actions Execution workspace. For more information, see [AI Desktop Actions Execution workspace](#).

Role required: `now_assist_panel_user`

About this task

The employee onboarding AI agent automates the complete workflow of onboarding new hires. When you invoke the agent, it executes a series of desktop actions.

Background task: Read Excel data

The agent opens the Excel file at the specified path and reads each row containing new hire information. This task runs silently without displaying the spreadsheet.

On-screen task: Create an HR record

The agent opens the HR system, navigates to the employee creation form, and fills each field with data from Excel (name, ID, department, manager). The agent

validates required fields and submits the form. You see the agent interacting with the form on the Windows desktop.

On-screen task: Provision email account

The agent navigates to the Microsoft 365 admin portal, creates a new user account with the employee's email address, and assigns the appropriate licenses. This step makes the email account immediately available.

On-screen task: Add to distribution list

The agent opens Microsoft Outlook, locates the team distribution list, and adds the new employee's email address as a member. This allows the employee to receive all team communications immediately upon activation.

Each action is orchestrated by the AI agent, which monitors completion and handles data transitions between steps. The entire workflow completes without manual intervention.

i Important: The AI agent executes desktop actions on a Windows machine. Do not interact with the desktop or keyboard during agent execution. The agent requires exclusive access to the Windows desktop to perform its tasks accurately.

Procedure

1. Prepare the new hire data in the designated Excel spreadsheet.
Verify that all required fields are populated: Employee Name, Employee ID, Department, Manager, and Email Address.
2. In ServiceNow, navigate to your HR requests or onboarding queue to confirm all new hire records are ready for processing.
3. Open the ServiceNow Otto panel by clicking the ServiceNow Otto  icon in the ServiceNow interface.
4. In the ServiceNow Otto panel, type: `Onboard new employees` or `Execute employee onboarding workflow`.

The AI agent recognizes your request and displays a prompt asking for:

- **Excel file path:** Location of the spreadsheet containing new hire data
- **HR system URL** (optional): Pre-configured if the agent already has access
- **Distribution list name:** The team or department distribution list to add employees to

5. Enter the required information and initiate execution.
6. Monitor the automation execution.

Automation execution process on ServiceNow Otto panel and AI Desktop Actions

On ServiceNow Otto panel	On AI Desktop Actions Execution workspace
The AI agent is triggered and starts preparing a plan.	The Execution workspace launches. The AI agent logs in. If this is the first time you launch the Execution workspace using AI agents, enter your Windows Security credentials when prompted.
The agent shows which desktop actions it uses for the execution.	The Execution workspace waits for instructions from AI Agent Studio.

On ServiceNow Otto panel	On AI Desktop Actions Execution workspace
The AI agent shows each step as it executes them.	The AI agent performs the tasks in the Execution workspace that shows the execution status. For more information, see AI Desktop Actions Execution workspace .
The outcome of the execution is shown in the ServiceNow Otto panel.	The Execution workspace returns to the ready state.

Note: If a pop-up window blocks the automation, select **Step in** to clear it, then select **Step out** to return control to the agent.

During execution, the agent uses the values configured for each input. Values can come from two sources: static values set during design time, or mapped parameter records. If you also specify values for inputs configured for parameters in the agent instructions or in the ServiceNow Otto panel, the mapped parameter values override them.

7. After the agent completes execution, verify successful onboarding by checking:

HR system

New employee records display in the employee list with all fields populated correctly.

Microsoft 365 Admin Portal

New employee accounts appear in the user list with assigned licenses and active status

Microsoft Outlook distribution list

New employees appear as members of the team distribution list

Exchange online

New employee mailboxes are provisioned and ready for use

Execution report in ServiceNow

The agent execution record shows all steps completed successfully with timestamps

8. If the agent encounters errors with specific employees, review the error details and resolve any data issues in the Excel spreadsheet or the target systems.

Common issues include:

- Missing data in Excel fields (all fields are required)
- Duplicate employee IDs in the HR system
- Invalid email format in the email field
- Distribution list name spelled incorrectly or list not accessible

9. For records that failed, resolve the issues and re-run the agent with corrected data. The agent will process only the failed records or you can re-run the complete batch.

10. **Optional:** Interact with the automation when your inputs are required.

- **Step in:** take control whenever human inputs are required
- **Step out:** give the control back to the AI agent.

Note: If your automation requires manual inputs, such as entering an OTP or CAPTCHA, you must provide instructions to the AI Agent to wait for the user input during execution. Otherwise, the automation can't proceed.

- 11. Optional:** Use the smart sizing options to enable your desktop executions automatically adapt to your display.

Option	Description
Fit to window	Scales the execution screen to fit within the display area of the Execution workspace. The entire screen is visible without scrolling. (Optional) Shortcut: <code>ctrl+shift+w</code>
Original resolution	Displays the execution screen at its original resolution. Scroll bars appear if the screen is larger than the display area of the Execution workspace. (Optional) Shortcut: <code>ctrl+shift+d</code>

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 Operational Sustainability Management's Sustainable IT

Feature	Hardware Asset Management	Operational Sustainability 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	✗	✗	✓

Feature	Hardware Asset Management	Operational Sustainability Management	All applications together
Track all relevant Sustainable IT metrics at a glance	✗	✗	✓

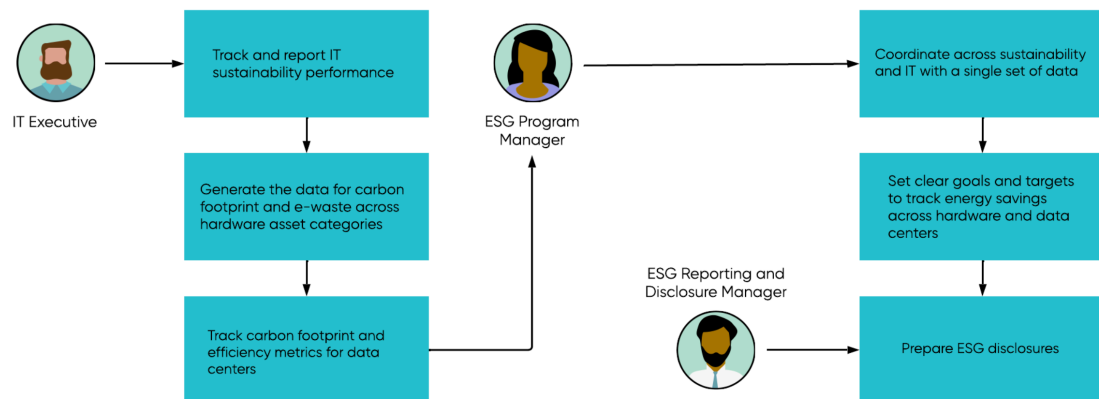
Workflow for using Hardware Asset Management and Sustainable IT

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 Operational Sustainability 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	✗	✓	✓

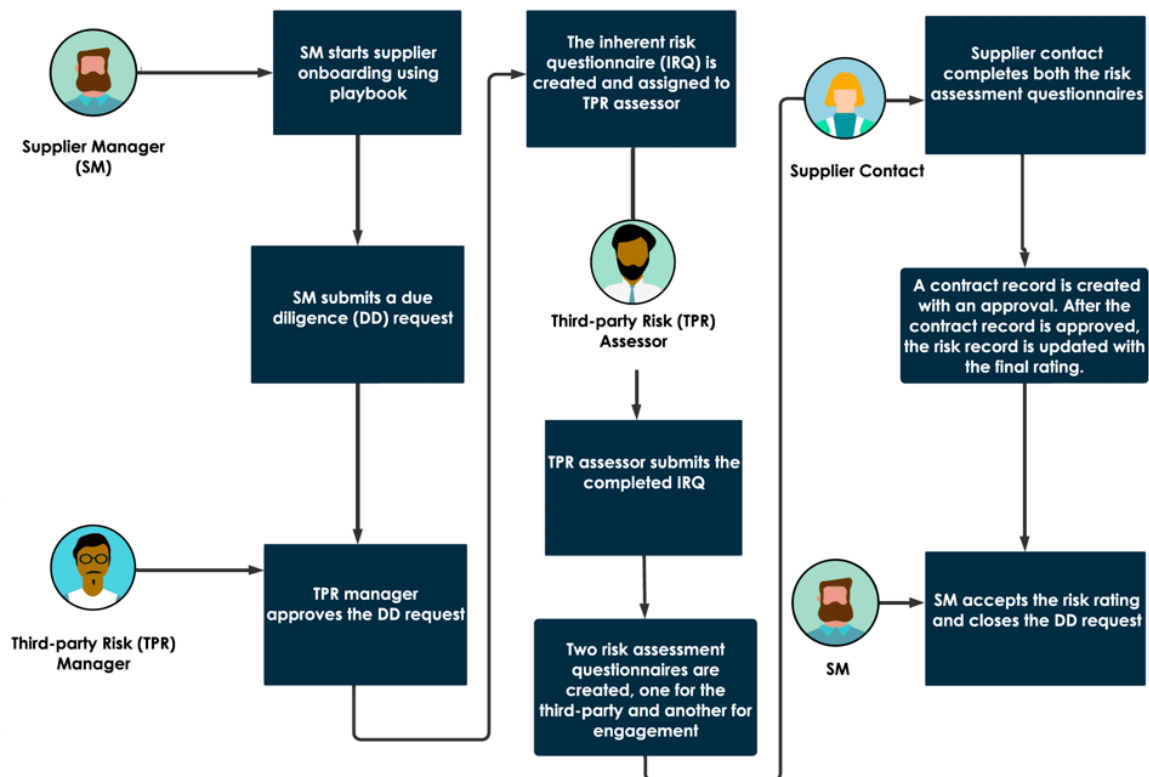
Workflow of Risk Assessments Integration for Supplier Lifecycle Operations

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



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 [Use the supplier onboarding playbook to onboard suppliers](#).
3. The supplier manager submits a due diligence request.

Performing due diligence 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 TPR manager approves the due diligence request.
5. The inherent risk questionnaire is created and assigned to the TPR assessor.
6. The TPR assessor submits the completed IRQ.
7. Two risk assessment questionnaires are created and assigned to the supplier contact.
8. The supplier contact logs in to the Supplier Collaboration Portal and completes the risk assessment questionnaires.
9. A contract record is created with an approval. After the contract record is approved, the risk record is updated with the final rating.
10. The supplier manager accepts the risk rating and closes the due diligence request.

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

1. Install the Supplier Lifecycle Operations (com.snc.sn_supplier_mgmt) application from the ServiceNow® Store. For more information, see [Install Supplier Case Management](#).
2. Install and activate the Risk Assessments Integration for Supplier Lifecycle Operations (com.snc.sn_supplier_tprm) plugin.
3. Install the Third-party Risk Management (com.sn_vdr_risk_asmt) application from the ServiceNow® Store. For more information, see [Configuring Third-party Risk Management](#).
4. Install and activate the GRC: Third-party Due Diligence Request (com.sn_tprm_onboarding) plugin.

Note: You must have a license for Third-party Risk Management (formerly Vendor Risk Management) to take advantage of this better together solution.

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 [Use the supplier onboarding playbook to onboard suppliers](#).
3. The playbook creates a due diligence request. For more information about the fields in this activity, see [Request due diligence for a third-party engagement](#).
4. The supplier manager fills and submits a due diligence request, which is assigned to the TPR manager.

Note: For each due diligence request, the system auto-assigns a unique ID number that starts with the prefix **DDR**.

5. If the due diligence request is approved by the TPR manager, the inherent risk questionnaire (IRQ) is sent to the TPR assessor (internal stakeholder).
6. After the TPR assessor submits the completed IRQ, the due diligence process begins.
7. The due diligence process creates two risk assessments, each containing an external due diligence questionnaire, one for the third-party and another for engagement.
8. After the supplier contacts complete and submit the external questionnaires from the Supplier Collaboration Portal, the TPR manager goes through the questionnaires and approves the due diligence request. For more information, see [Complete a risk assessment from the Supplier Collaboration Portal](#).
9. A contract record is created with an approval. After the contract record is approved, the risk record is updated with the final rating.
10. After the supplier manager accepts the risk rating, an email is sent to the requester informing that the due diligence request has been successfully processed and approved.
11. The supplier manager closes the due diligence request (case).
12. As a supplier manager, you can use the risk assessment result data in combination with any other data to determine whether to continue or cancel the onboarding process.

Enhancing the asset procurement experience using IT Asset Management (ITAM) and Sourcing and Procurement Operations (SPO)

Integrating IT Asset Management (ITAM) with Sourcing and Procurement Operations (SPO) enhances the procurement process for service requests.

Combined benefits of integrating IT Asset Management and Sourcing and Procurement Operations

Integrating ITAM with SPO provides the following benefits:

- Streamlines workflows and improves the experience for asset managers and end users.
- Enables asset managers to initiate and manage external purchases directly from ITAM.
- Improves data integrity and compliance through synchronized records.
- Delivers faster, asset-driven procurement with fewer manual steps.
- Manages receipts, shipments, and assets automatically and consistently across Asset Management (ALM) and SPO.

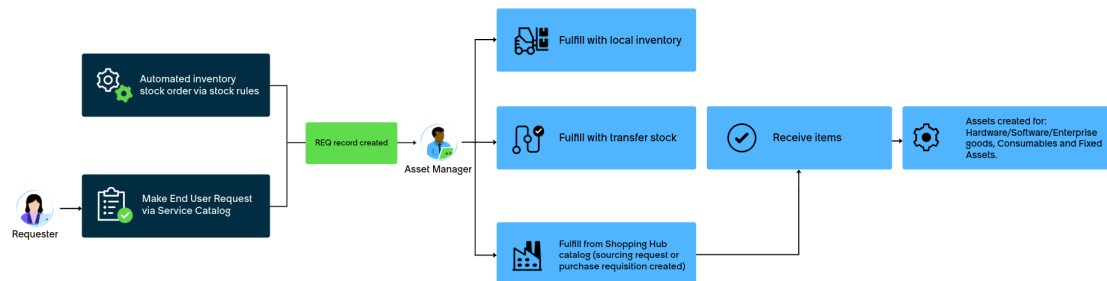
Feature	IT Asset Management	Sourcing and Procurement Operations	All applications together
Raise sourcing requests for catalog items without a price	✗	✓	✓
Generate purchase requests for catalog items with a price	✗	✓	✓
Submit asset requests from Employee Center or Service Catalog	✓	✗	✓
Create requests via stock replenishment rules	✓	✗	✓
Receive assets using mobile barcode scanning	✓	✗	✓
Generate comprehensive records in the Asset [alm_asset], Software License [alm_license], and Consumable [alm_consumable] table	✓	✗	✓

Workflow for IT Asset Management and Sourcing and Procurement Operations better together feature

Using the IT Asset Management and Sourcing and Procurement Operations applications together provides the following benefits:

- Create and manage external purchase by accessing the items from the Shopping Hub within the IT Asset Management application.
- Manage all related receipts and shipments automatically and consistently across IT Asset Management and Sourcing and Procurement Operations applications.

The IT Asset Management and Sourcing and Procurement Operations workflow



In this workflow:

1. The procurement journey begins with one of the following events:
 - An employee requests IT assets through the Service Catalog.
 - An automated inventory stock order is generated based on stock rule configurations.
2. The Procurement Manager checks whether the request can be fulfilled with items from local stock, by transferring items, or by placing an order.
3. The Procurement Manager with the following roles can create a Purchase Order by accessing the items with or without a price from the Shopping Hub catalog to fulfill the service request.
 - procurement_admin or procurement_user
 - asset manager role (sn_spend_asset.spo_shopper)
4. After the Purchase Order is completed, the requested assets are received and delivered to the stockroom.
5. In the IT Asset Management application, assets are created when you confirm receipt of the requested items. Depending on the type of the asset, one of the following asset records is created:
 - For hardware or enterprise assets, a record is added to the Asset [alm_asset] table.
 - For software assets, an entitlement is created in the Software License [alm_license] table.
 - For consumable assets, an entitlement is created in the Consumable [alm_consumable] table.

Requirements for integrating IT Asset Management and Sourcing and Procurement Operations

The following plugins are required to use the IT Asset Management Integration for Sourcing and Procurement Operations better together feature:

1. IT Asset Management Integration for Sourcing and Procurement Operations (com.snc.sn_spend_asset) plugin
2. Sourcing and Purchasing Automation (com.snc.sn_pr) plugin
3. Procurement (com.snc.procurement) plugin
4. Shopping Hub (com.snc.uib.sn_spend_uib) plugin

The following additional plugins are required based on the specific IT Asset Management products installed:

- Enterprise Asset Management (com.sn_eam) plugin
- Hardware Asset Management (com.sn_hamp) plugin
- Software Asset Management (com.snc.samp) plugin

Get started with procuring assets from the Shopping Hub catalog

Start procuring assets by accessing the items from the Shopping Hub catalog by completing these tasks:

1. [Activate Asset Management Integration for Sourcing and Procurement Operations \(sn_spend_asset\) plugin](#).
2. Begin sourcing and procuring of the requested items from the IT Asset Management workspaces such as Software Asset Workspace, Hardware Asset Workspace, or Enterprise Asset Workspace. For more information, see [Create Sourcing Request or Purchase Requisition in SPO via IT Asset Management workspace](#).
3. Receive the requested assets in a stockroom. For more information, see [Receiving assets in the IT Asset Management](#) application.
4. Acknowledge the receipt of the assets in the stockroom for asset creation. For more information, see [Asset creation in the IT Asset Management application](#).