servicenow

Yokohama – Besser gemeinsam

Zuletzt aktualisiert: 17.12.2025

Automatische Übersetzung

Diese Materialien wurden für Sie mit einer Übersetzungssoftware übersetzt. Es wurden angemessene Anstrengungen unternommen, um Ihnen eine akkurate Übersetzung zu liefern. Jedoch können menschliche Übersetzer nicht durch automatisierte Übersetzungstechnologien ersetzt werden. Die Übersetzungen werden ungeprüft bereitgestellt. Es wird keinerlei Gewährleistung, weder ausdrücklich noch implizit, für die Genauigkeit, Zuverlässigkeit und Richtigkeit von Übersetzungen in andere Sprachen übernommen. Manche Inhalte wurden aufgrund der Beschränkungen der Übersetzungssoftware möglicherweise nicht präzise übersetzt. Die Ausgangssprache dieser Dokumente ist Englisch. Jegliche Diskrepanzen oder Unterschiede, die bei der Übersetzung entstehen, sind nicht verbindlich und haben keine Rechtswirkung für die Einhaltung oder Durchsetzung von Rechten.

Einige Beispiele und Grafiken, die hier dargestellt sind, dienen nur der Veranschaulichung.®ine echte Zuordnung oder Verbindung zu ServiceNow-Produkten oder -Services ist nicht beabsichtigt und sollte nicht abgeleitet werden.

Bitte lesen Sie die Nutzungsbedingungen für die ServiceNow-Website unter www.servicenow.com/terms-of-use.html

Automatische Übersetzung

Firmensitz
2225 Lawson Lane
Santa Clara, CA 95054
USA
(408) 501-8550

Inhaltsverzeichnis

Lösungen

Mit Lösungen können Sie die Funktionalität von ServiceNow -Anwendungen verbessern, indem Sie sie in Kombination miteinander verwenden.

Verfügbare Lösungen

Erfahren Sie mehr über die Vorteile der einzelnen Lösungen und wie Sie sie implementieren und verwenden können.

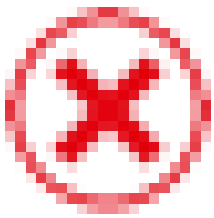
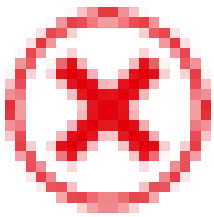
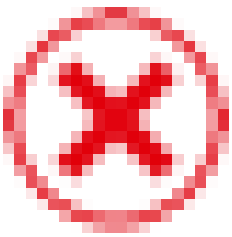
Verbessern Sie die Transparenz des organisatorischen Risikos mit der erweiterten Bewertung des Projektrisikos

Mit der erweiterten Risikobewertung für Ihre Projekte können Sie leicht erkennen, ob Projekte potenzielle organisatorische Risiken bergen, und schnell über entschärfende Maßnahmen entscheiden. Kombinieren Sie Projektrisikomanagement mit Enterprise-Risikomanagement, um einen besseren Einblick in die Gesamtrisiken Ihrer Organisation zu erhalten.

Kombinationsvorteile der Integration von Projekt-Portfoliomanagement mit Erweitertes Risikomanagement

Funktion	Projekt-Portfoliomanagemen	Erweitertes Risikomanagement	Beide Anwendungen gleichzeitig
Projektrisikobewertung	✓	✗	✓
Wird auf Unternehmensrisiko hochgestuft	✗	✗	✓
Bewertung von inhärenten und Restrisiken	✓	✓	✓
Integrierte Projekt- und Unternehmensrisikoregister	✗	✗	✓

Automatische Übersetzung

Funktion	Projekt-Portfoliomanagemen	Erweitertes Risikomanagement	Beide Anwendungen gleichzeitig
Risiko-Heatmaps			
Risikoübersichts-Dashboard für Enterprise-Projekte			

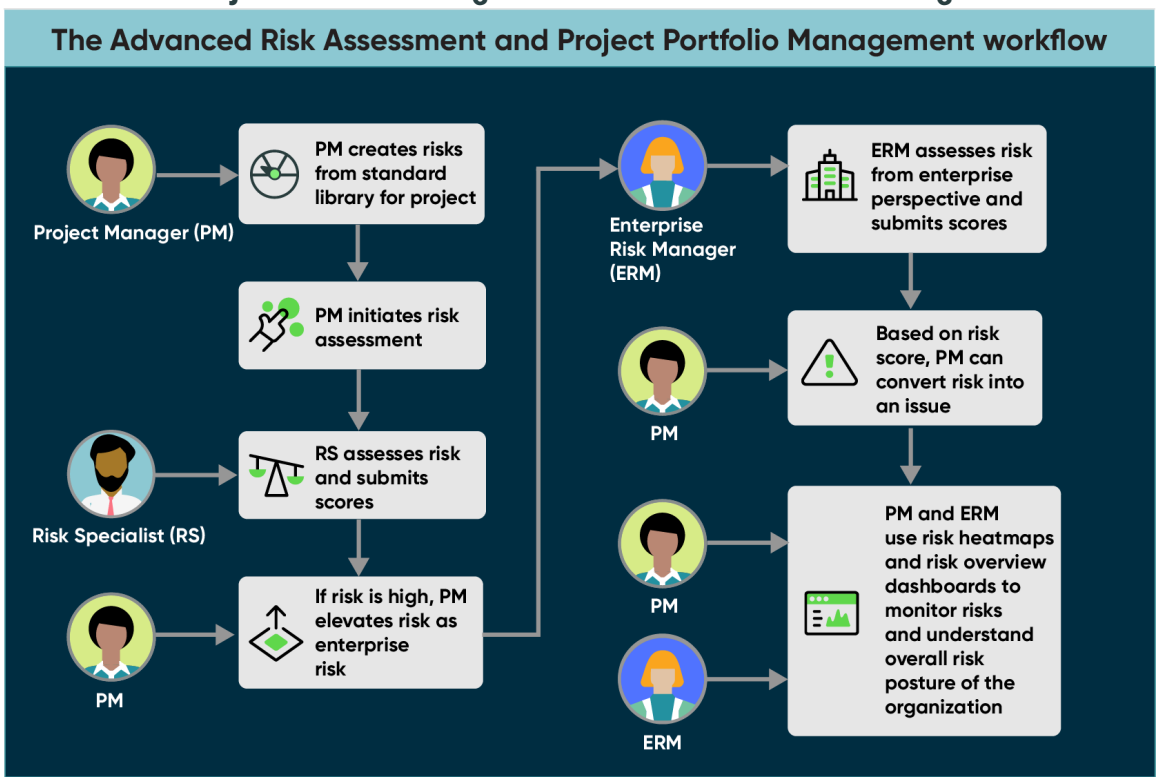
Workflow der erweiterten Projektrisikobewertung

Verwenden Sie Projekt-Portfoliomanagement (PPM) und Erweitertes Risikomanagement Assessment (ARA) zusammen für die folgenden Vorteile:

- Überwachen Sie Ihre Risiken auf Organisationsebene
- Integrieren Sie Ihr Risikomanagementsystem für Projekt- und Enterprise-Risikoteams.

Die folgende Abbildung zeigt einen Beispiel-Workflow, der zeigt, wie ein Projektmanager, ein Risikospezialist und ein Enterprise-Risikomanager die Anwendungen gemeinsam verwenden, um Risiken auf Projekt- und Unternehmensebene zu bewerten und zu minimieren.

Der Workflow Projekt-Portfoliomanagement und Erweitertes Risikomanagement .



In diesem Workflow:

1. Der Projektmanager erstellt Risiken aus der Standardbibliothek für das Projekt und initiiert dann die Risikobewertung.
2. Der Risikospezialist bewertet das Risiko und vergibt eine Bewertungspunktzahl.
3. Wenn die Risikopunktzahl hoch ist, erhöht der Projektmanager das Risiko als Unternehmensrisiko.
4. Der Enterprise-Risikomanager bewertet das Risiko aus der Unternehmensperspektive und vergibt eine Bewertungspunktzahl.
5. Basierend auf der Risikopunktzahl kann der Projektmanager das Risiko in ein Problem umwandeln.
6. Der Projektmanager und der Enterprise-Risikomanager verwenden Risiko-Heatmaps und Risikoübersichts-Dashboards, um die Risiken zu überwachen und die allgemeine Risikosituation des Unternehmens zu verstehen.

Anforderungen für die Integration Projekt-Portfoliomanagement von und Erweitertes Risikomanagement .

1. Aktivieren Sie das Plugin „Project Portfolio Management“ [com.snc.financial_planning_pmo].
2. Installieren Sie die Anwendung GRC: Advanced Risk aus ServiceNow® Store.

Erste Schritte mit der erweiterten Risikobewertung von Projekten

Führen Sie die folgenden Schritte aus, um mit der Bewertung von Projektrisiken zu beginnen:

1. Richten Sie die Risikobewertungsmethode ein und konfigurieren Sie sie. Weitere Informationen finden Sie unter Projekt-Portfoliomanagement und Integration für erweitertes Risikomanagement konfigurieren .

   Rolle: sn_risk.admin.

2. Definieren Sie den Umfang, und initiieren Sie die Risikobewertung. Weitere Informationen finden Sie unter Risiken für ein Projekt hinzufügen .

   Rolle: it_project_manager.

3. Führen Sie eine Risikobewertung durch. Weitere Informationen finden Sie unter Risikobewertung durchführen .

   Rolle: sn_grc.business_user

4. Bewerten und auf Projektrisiko erhöhen. Weitere Informationen finden Sie unter Projektrisiko zu Unternehmensrisiko hochstufen .

   Rolle: it_project_manager.

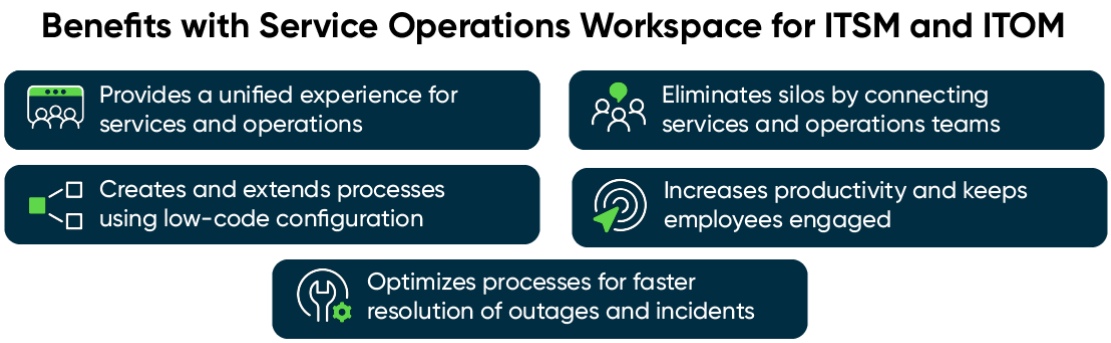
5. Konvertieren Sie Risiken in Probleme, und überwachen Sie die Sicherheitslage. Weitere Informationen finden Sie unter Risikosituation überwachen .

   Rolle: sn_risk.admin, it_project_manager.

Automatisieren und optimieren Sie Ihre Services und Vorgänge mit Service Operations-Arbeitsbereich

Sie können Services erweitern und gleichzeitig Kosten senken, qualitativ hochwertige Kunden- und Mitarbeiter-Experiences bieten und die organisationale Resilienz steigern. Verwenden Sie eine einzige Cloud-Plattform, die IT-Prozesse wie Incidents, Probleme und Changes mit IT-Vorgängen wie Discovery, Business Service-Definitionen, Service-Mapping und Event Management integriert.

Kombinationsvorteile der Integration von Service Operations-Arbeitsbereich für IT Service Management (ITSM) und IT Operations Management (ITOM)



Funktion	Service Operations-Arbeitsbereich für ITSM	Service Operations-Arbeitsbereich für ITOM	Alle Anwendungen auf einmal
Einfache, intuitive und übersichtliche Benutzeroberfläche (UI)	✓	✓	✓
Automatisierte Empfehlungen basierend auf Benutzeraktionen	✓	✓	✓
Maßgeschneiderte Zielseite, die eine Übersicht über Aufgaben bietet	✓	✓	✓
Effektives Incident-Management für Service Desk-Mitarbeiter	✓	✗	✓
Experten in Rufbereitschaft für Aufgaben mit hoher Priorität	✓	✗	✓
Onboarding-Experience für angemeldete Benutzer	✓	✓	✓
Walk-Up Experience	✓	✗	✓
Anforderungsmanagement aus Incidents und Interaktionen	✓	✗	✓

Automatische Übersetzung

Funktion	Service Operations-Arbeitsbereich für ITSM	Service Operations-Arbeitsbereich für ITOM	Alle Anwendungen auf einmal
Geführte Experience für die Erstkonfiguration von Service Operations-Arbeitsbereich	✓	✗	✓
Darstellung des vollständigen Kontexts eines Service mit zugehörigen Metriken, Protokollen und zusätzlichen Informationen	✗	✓	✓
Schnelle Nachbesserung für Warnungen eines Service	✗	✓	✓
Schnelle Automatisierung für Bediener, wenn sie eine eingebettete Playbook-Experience innerhalb der Warnungsformulare verwenden	✗	✓	✓

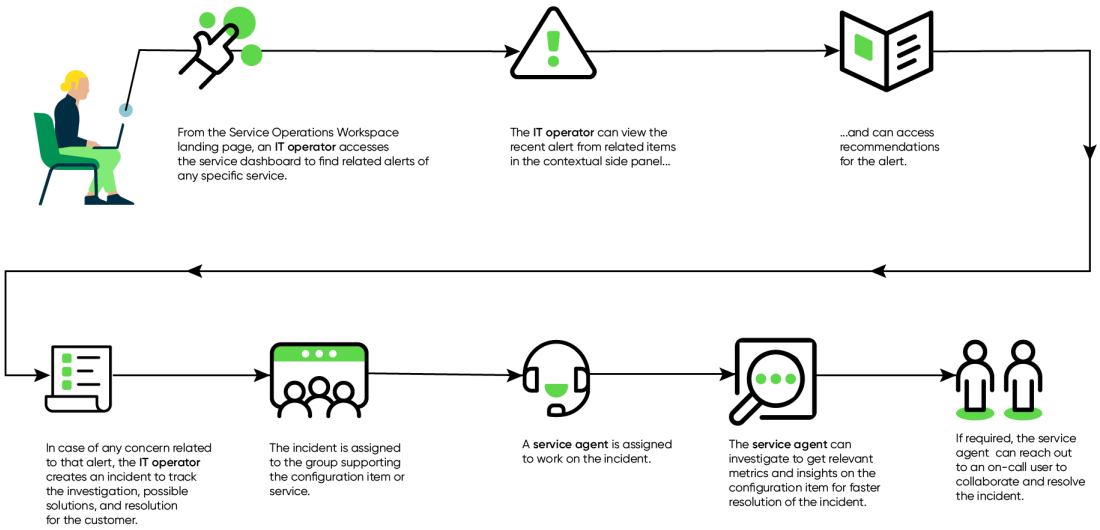
Workflow für Service Operations-Arbeitsbereich

Verwenden Sie Service Operations-Arbeitsbereich für IT Service Management (ITSM) und IT Operations Management (ITOM) zusammen für die folgenden Vorteile:

- Bieten Sie eine einheitliche Experience für Services und Vorgänge auf einer einzigen Plattform.
- Beseitigen Sie Silos, indem Sie Service- und Betriebsteams verbinden.
- Steigern Sie die Produktivität, und binden Sie die Mitarbeiter ein.
- Erstellen und erweitern Sie die Prozesse ITSM und ITOM mit Low-Code-Konfiguration.
- Optimieren Sie die Prozesse ITSM und ITOM für eine schnellere Lösung von Incidents und Ausfällen.

Die folgende Abbildung zeigt einen Beispiel-Workflow, der zeigt, wie ein IT-Mitarbeiter und ein Servicemitarbeiter (Service Desk-Mitarbeiter oder L2/L3-Spezialist) diese Anwendungen verwenden können, um ein Kundenproblem zu lösen.

Service Operations-Arbeitsbereich für Workflow ITSM und ITOM .



In diesem Workflow:

1. Über die Zielseite Service Operations-Arbeitsbereich greift ein IT-Operator auf das Service-Dashboard zu, um zugehörige Warnungen zu einem bestimmten Service zu finden.
2. Der IT-Bediener kann die letzte Warnung aus zugehörigen Elementen im kontextbezogenen Seitenbereich anzeigen.
3. Der IT-Mitarbeiter kann auf Empfehlungen für die Warnung zugreifen.
4. Wenn im Zusammenhang mit dieser Warnung ein Kundenproblem vorliegt, erstellt der IT-Betreiber einen Incident, um die Untersuchung, mögliche Lösungen und die Lösung für den Kunden nachzuverfolgen.
5. Der Incident wird der Gruppe zugewiesen, die das Configuration Item oder den Service unterstützt.
6. Ein Servicemitarbeiter wie ein Service Desk-Mitarbeiter oder L2/L3-Spezialist wird zur Bearbeitung des incident zugewiesen.
7. Der Servicemitarbeiter kann untersuchen, um relevante Metriken und Einblicke in das Konfigurationselement zu erhalten und den Incident schneller zu lösen.
8. Bei Bedarf kann der Service-Mitarbeiter einen Benutzer in Rufbereitschaft kontaktieren, um die Zusammenarbeit und die Lösung des incident zu unterstützen.

Anforderungen für die Integration von Service Operations-Arbeitsbereich für ITSM und ITOM

1. Stellen Sie sicher, dass die folgenden Bedingungen für Service Operations-Arbeitsbereich für ITSMerfüllt sind.
   a. Erwerben Sie eine Standardlizenz ITSM oder höher für Anwendungen ServiceNow® IT Service Management. Wenden Sie sich an Ihren Account Manager oder Vertriebsmitarbeiter für ServiceNow.
   b. Wenn Sie das Untersuchungs-Framework in Service Operations-Arbeitsbereich für ITSMverwenden möchten, erwerben Sie die Lizenz ITSM Professional oder höher für ServiceNow® IT Service Management -Anwendungen.
   c. Installieren Sie Service Operations-Arbeitsbereich ITSM Anwendungen aus dem ServiceNow® Store. Informationen zur Installation dieser Anwendung finden Sie unter ITSM-Anwendungen für den Service Operations-Arbeitsbereich installieren.
2. Stellen Sie sicher, dass die folgenden Bedingungen für Service Operations-Arbeitsbereich für ITOMerfüllt sind.
   a. Erwerben Sie eine ITOM Professional-Lizenz oder höher für ServiceNow® IT Operations Management -Anwendungen. Wenden Sie sich an Ihren Account Manager oder Vertriebsmitarbeiter für ServiceNow.
   b. Installieren Sie Service Operations-Arbeitsbereich ITOM Anwendungen aus dem ServiceNow® Store. Informationen zur Installation dieser Anwendung finden Sie unter Service Operations-Arbeitsbereich für ITOM-Anwendungen installieren .

Erste Schritte mit Service Operations-Arbeitsbereich für ITSM und ITOM

Führen Sie die folgenden Schritte aus, um Service Operations-Arbeitsbereich für ITSM und ITOMzu verwenden:

1. Konfigurieren Sie Service Operations-Arbeitsbereich für ITSM.
   a. Richten Sie Service Operations-Arbeitsbereich für ITSMein. Weitere Informationen finden Sie unter Service Operations-Arbeitsbereich für ITSM einrichten.

      Rolle: admin.

   b. Richten Sie das Untersuchungs-Framework ein. Weitere Informationen finden Sie unter Untersuchungs-Framework im Service Operations-Arbeitsbereich einrichten .

      Rolle: admin.

   c. Konfigurieren Sie das Empfehlungs-Framework für einen Incident. Weitere Informationen finden Sie unter Empfehlungs-Framework in Service Operations-Arbeitsbereich für ITSM konfigurieren .

      Rolle: admin.

2. Konfigurieren Sie Service Operations-Arbeitsbereich für ITOM.
   a. Richten Sie Service Operations-Arbeitsbereich für ITOMein. Weitere Informationen finden Sie unter Service Operations-Arbeitsbereich für ITOM einrichten.

      Rolle: evt_mgmt_operator.

b. Konfigurieren Sie Warnungsmetriken. Weitere Informationen finden Sie unter Warnungsmetriken konfigurieren .

Rolle: evt_mgmt_operator.

c. Konfigurieren Sie das Empfehlungs-Framework für eine Warnung. Weitere Informationen finden Sie unter Empfehlungs-Framework in Service Operations-Arbeitsbereich für ITOM konfigurieren.

Rolle: evt_mgmt_admin

d. Konfigurieren Sie den Posteingang Service Operations-Arbeitsbereich. Weitere Informationen finden Sie unter Posteingang in Service Operations-Arbeitsbereich für ITOM konfigurieren.

Rolle: evt_mgmt_admin

e. Passen Sie Service Operations-Arbeitsbereich -Listen an. Weitere Informationen finden Sie unter Listen in Service Operations-Arbeitsbereich für ITOM anpassen .

Rolle: itil

Fallstudie: Verbesserung von Risiko, Compliance und Audit-Management mit ITOM

Der Anwendungsfall zeigt, wie die ITOM -Integration das Risiko-, Compliance- und Audit-Management für ein Finanzinstitut optimiert, indem sie für Echtzeit-Transparenz, Automatisierung und verbesserte Risikobewertungen sorgt.

Kurzbeschreibung des Problems

Ein führendes Finanzinstitut versucht, seine Risikomanagementprozesse zu optimieren, um die immer komplexer werdenden Betriebs-, Drittpartei- und Technologierisiken sowie Compliance- und interne Audit-Funktionen zu verwalten. Die Institution erkannte die Notwendigkeit einer einheitlichen Plattform, um die Effizienz zu verbessern und den manuellen Aufwand zu reduzieren.

Herausforderungen

- Mangel an zentralisierter Transparenz: Das Finanzinstitut stand vor der Herausforderung, eine klare Echtzeitansicht von Risiko-, Compliance- und Audit-Prozessen zu erhalten. Unterschiedliche Systeme erschweren die Bewertung von Betriebsrisiken im Zusammenhang mit IT-Services und Infrastruktur.
- Isolierte IT-Infrastruktur: Die getrennten IT-Systeme der Institution machten es schwierig, operative Probleme zu überwachen und darauf zu reagieren, die sich auf Risikomanagementfunktionen auswirken könnten, z. B. Ausfallzeiten, Konfigurationsfehler und Ausfälle von IT-Services.
- Eingeschränkte Nutzung vorhandener Daten: Die erhebliche Menge an IT-Daten, die aus verschiedenen Quellen verfügbar sind, wurde aufgrund der fehlenden Integration in vorhandene Systeme nicht vollständig für das Risiko- und Compliance-Management genutzt.

ITOM-spezifische Lösungen

- Operative Echtzeittransparenz: ITOM verschaffte der Einrichtung Echtzeiteinblicke in den Zustand, die Verfügbarkeit und die Leistung von IT-Services. Durch die Integration ITOM von in ServiceNow IRMkonnten Risiko- und Compliance-Teams Betriebsrisiken (z. B. Serviceausfälle, Leistungsverschlechterungen) direkt mit umfassenderen Risikomanagementbemühungen korrelieren.
- Automatisiert Service-Mapping für bessere Risikobewertung: Die Fähigkeiten Service-Mapping in ITOM ermöglichten es der Institution, IT-Services automatisch abzubilden und ihre Abhängigkeiten zu verstehen. Dies war entscheidend für die Bewertung von Betriebsrisiken in Echtzeit. Beispielsweise könnte das System einen kritischen Servicefehler erkennen und ihn im Compliance-Dashboard sofort als Ereignis mit hohem Risiko kennzeichnen, sodass die Institution vorbeugende Maßnahmen ergreifen kann.
- Proaktive Überwachung und Reaktion auf Warnungen: Durch den Einsatz von ITOM Ereignismanagementkonnte die Institution wichtige Betriebsrisiken wie Systemausfälle und Ausfälle von Drittparteiservices überwachen und automatisierte Warnungen an relevante Risikomanagement- und Compliance-Teams senden. Dieser proaktive Ansatz minimierte die Zeit zwischen der Identifizierung eines Betriebsrisikos und der Reaktion darauf.
- Configuration Management Database (CMDB) für Compliance: Die Integration von ITOM mit CMDB stellte sicher, dass alle IT-Assets, Konfigurationen und ihre Beziehungen genau nachverfolgt wurden. Dadurch wurde eine einzige wahrheitsgemäße Quelle für das Risikomanagement bereitgestellt, mit der Compliance-Teams Risiken automatisch mit bestimmten IT-Assets oder Services verknüpfen konnten, um genauere Risikobewertungen sicherzustellen, insbesondere im Kontext von Technologierisiken und Drittparteiabhängigkeiten.
- Reduzierung des Warnungsrauschens und Automatisierung: ITOM AIOps wurde genutzt, um die Ermüdung von Warnungen zu reduzieren, indem zugehörige Warnungen (z. B. aufgrund von Infrastrukturfehlern) automatisch gruppiert und korreliert werden. Dadurch wurde der manuelle Aufwand für Risiko- und Compliance-Teams beim Sichten irrelevanter Warnungen reduziert, sodass sie sich auf Betriebsrisiken mit höherer Priorität konzentrieren können.

Schlüsselergebnisse

- Einheitliche Risiko- und IT-Vorgänge: Durch die Integration von ITOM in ServiceNow IRMerreichte die Institution eine einheitliche Ansicht der Betriebs- und IT-Risiken. Diese Integration erleichterte die Identifizierung von Risiken, die sich aus operativen IT-Fehlern ergeben, und unterstützte die Einrichtung dabei, kritische Warnungen schnell zu beheben, bevor sie eskalieren.
- Höhere Effizienz durch Automatisierung: Die Automatisierung ITOM von hat der Institution geholfen, manuelle Prozesse im Zusammenhang mit der Überwachung von Betriebsrisiken zu eliminieren, z. B. die manuelle Nachverfolgung von Serviceunterbrechungen oder Changes in der IT-Umgebung, die neue Risiken mit sich bringen könnten.
- Verbesserte Compliance mit IT-bezogenen Vorschriften: Die von ITOM bereitgestellten Echtzeitdaten stellten sicher, dass die Institution die gesetzlichen Anforderungen in Bezug auf IT-Risiken und Audit-Bereitschaft erfüllen konnte. Durch die Fähigkeit von ITOM, alle IT-Assets und -Konfigurationen auf dem neuesten Stand zu halten, wurden Audit-Prozesse schneller und genauer durchgeführt.
- Skalierbarkeit für zukünftige Risikomanagementanforderungen: Die native Cloud-Architektur von ITOM sorgte für Skalierbarkeit und Flexibilität und stellte sicher, dass

die Institution Risiken auch bei Wachstum verwalten konnte. ITOM unterstützte auch den mobilen Zugriff, was die Remote-Überwachung und das Warnungsmanagement durch Risiko- und IT-Teams ermöglichte.

Leistung Ihrer IT-Assets mit Hardware Asset Management und Nachhaltige ITnachverfolgen

Mit der Anwendung Nachhaltige IT können Sie die von Ihren Hardware-Assets erzeugten Emissionen effektiv verwalten und überwachen. Darüber hinaus können Sie den Energieverbrauch Ihrer Assets und deren ordnungsgemäße Entsorgung nach dem Ende ihrer Lebensdauer nachverfolgen.

Kombinierte Vorteile der Integration von Hardware Asset Management und ESG Managements Nachhaltige IT

Funktion	Hardware Asset Management	ESG Management	Alle Anwendungen auf einmal
Inventarmanagement für Hardware-Assets	✓	✗	✓
Energieverbrauch und Emissionen von Hardware-Assets schätzen	✗	✓	✓
Nachverfolgung des Lebenszyklus von Hardware-Assets	✓	✗	✓
Reduzierung von Elektroschrott melden	✗	✓	✓
Erhöhen Sie den Anteil der Energy Star-zertifizierten Assets im Portfolio	✗	✗	✓

Automatische Übersetzung

Funktion	Hardware Asset Management	ESG Management	Alle Anwendungen auf einmal
Verfolgen Sie den Energieverbrauch, CO2-Ausstoß und die Erneuerbaren Energien des Rechenzentrums	✗	✓	✓
Überwachen Sie PUE, WUE und CUE von jedem Standort aus im Hinblick auf gezielte Verbesserungen	✗	✗	✓
Verfolgen Sie alle relevanten Metriken zu Nachhaltiger IT auf einen Blick	✗	✗	✓

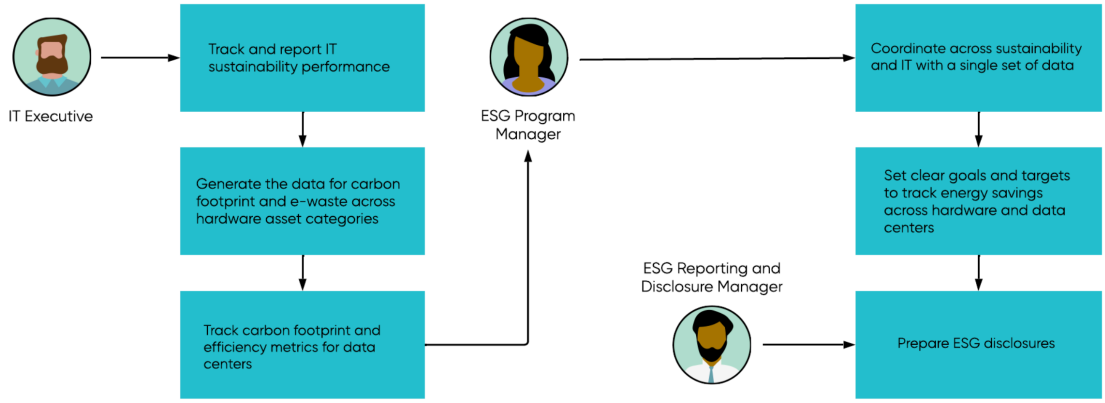
Workflow für die Verwendung Hardware Asset Management von und Nachhaltige IT

Die gleichzeitige Verwendung der Anwendungen Hardware Asset Management und Nachhaltige IT bietet folgende Vorteile:

- Ermöglicht Ihnen, die von Ihren Hardware-Assets erzeugten Emissionen effektiv zu verwalten und zu überwachen
- Hilft Ihnen, den Energieverbrauch Ihrer Assets und deren ordnungsgemäße Entsorgung nachzuverfolgen, nachdem sie das Ende ihrer Lebensdauer erreicht haben.
- Bietet über ein Dashboard wertvolle Einblicke, mit denen Sie fundierte Entscheidungen darüber treffen können, ob diese Assets stillgelegt oder neu verwendet werden sollen

Die Abbildung veranschaulicht die Zusammenarbeit zwischen einer IT-Verantwortlichen und dem Sustainability-Programmmanager bei der Erfassung von Daten zum CO2-Fußabdruck und zu Elektroschrott. Die ESG-Programmmanager legen Ziele und Zielvorgaben fest, um die Effizienz von Energiesparmaßnahmen zu überwachen und Offenlegungen vorzubereiten.

Der Workflow Hardware Asset Management und Nachhaltige IT .



In diesem Workflow:

1. Die IT-Verantwortliche meldet sich beim Asset-Arbeitsbereich für Führungskräfte an, um die IT-Nachhaltigkeitsleistung nachzuverfolgen und entsprechende Berichte zu erstellen.
2. Die IT-Verantwortliche ruft dann den CO2-Fußabdruck und den erzeugten Elektroschrott in verschiedenen Hardware-Asset-Kategorien ab und verfolgt den CO2-Fußabdruck und die Effizienzmetriken für Rechenzentren.
3. Der ESG-Programmmanager koordiniert Nachhaltigkeit und IT mit einem einzigen gemeinsamen Datensatz.
4. Die ESG-Programmmanager legen Ziele und Zielvorgaben fest, um die Effizienz von Energiesparmaßnahmen zu überwachen und so den ESG-Berichterstellungs- und Offenlegungsmanager bei der Vorbereitung der Offenlegungen zu unterstützen.
5. Der ESG-Reporting- und Offenlegungsmanager erstellt die ESG-Offenlegungen.

Anforderungen für die Integration Hardware Asset Management von und ESG Management

1. Installieren und aktivieren Sie das Plugin Nachhaltige IT (sn_esg_sustain).
2. Installieren und aktivieren Sie das Plugin Hardware Asset Management (sn_hamp).

Erste Schritte mit Nachhaltige IT, um die Emissionsdaten Ihrer IT-Assets nachzuverfolgen

Beginnen Sie mit Nachhaltige IT, indem Sie die folgenden Aufgaben ausführen:

1. Activate the Sustainable IT plugin .
2. Filtern und aktivieren Sie die Metrikdefinitionen für Nachhaltige IT .
3. Create new entities for data centers .
4. Manually set up entities for Sustainable IT data centers .
5. Configure Sustainable IT .

Minimieren Sie das Risiko, indem Sie Lieferanten während des Onboarding-Prozesses bewerten

Mit der Integration von Risikobewertungen für Supplier Lifecycle Operationskönnen Sie potenzielle Lieferantenrisiken beim Onboarding neuer Lieferanten identifizieren und bewerten.

Kombinationsvorteile der Integration von Supplier Lifecycle Operations mit Risikomanagement von Drittparteien

Funktion	Supplier Lifecycle Operations	Risikomanagement von Drittparteien	Alle Anwendungen auf einmal
Lieferanten-Onboarding	✓	✗	✓
Informations- und Datenverwaltung	✓	✗	✓
Fall- und Konfliktmanagement	✓	✗	✓
Risiko-Onboarding	✗	✓	✓
Drittpartei-Risiko-Sorgfaltspflicht, Bewertung externer und interner Risiken	✗	✓	✓

Automatische Übersetzung

Funktion	Supplier Lifecycle Operations	Risikomanagement von Drittparteien	Alle Anwendungen auf einmal
Risk Intelligence	✗	✓	✓
Risikobewertung und -überwachung	✗	✓	✓
Risikomanagement-Dashboard	✗	✓	✓

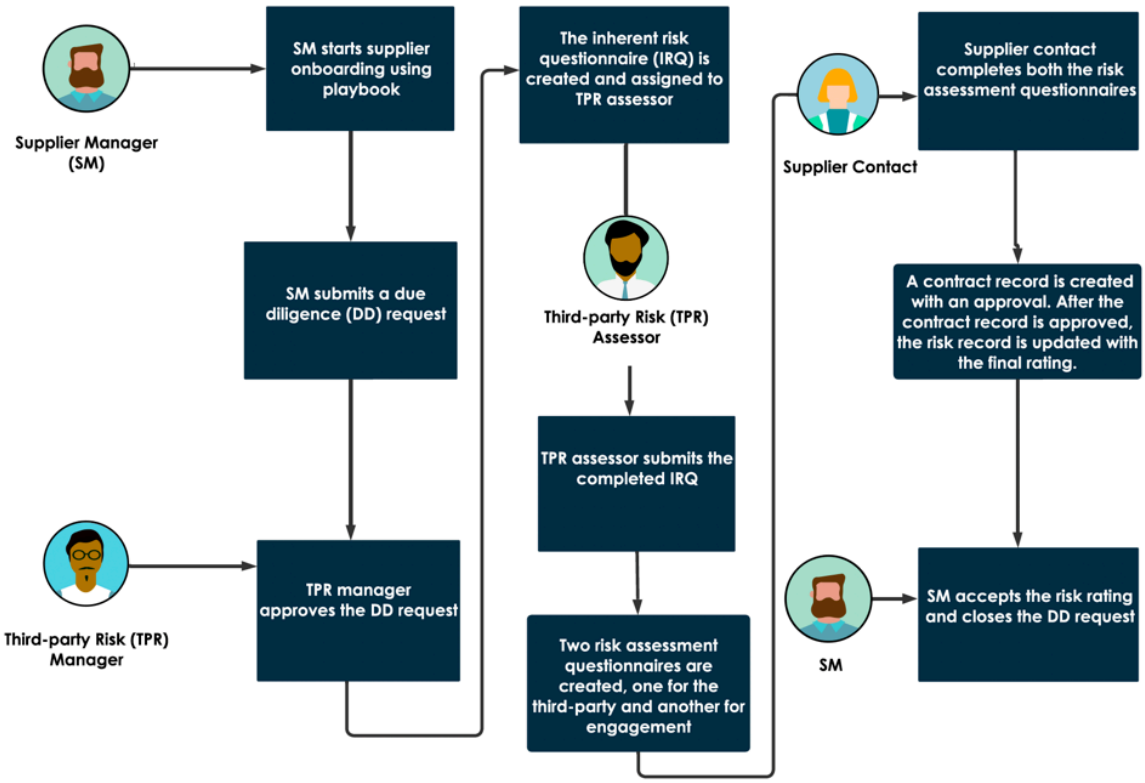
Workflow der Risikobewertungsintegration für Supplier Lifecycle Operations

Verwenden Sie Supplier Lifecycle Operations und Risikomanagement von Drittparteien zusammen für diese Vorteile:

- Bewerten Sie das Lieferantenrisiko beim Onboarding von Lieferanten
- Analysieren Sie die Risikopunktzahl, um zu bestimmen, ob ein Lieferant hinzugezogen werden soll

Die folgende Abbildung zeigt einen Beispiel-Workflow, der zeigt, wie ein Lieferantenmanager und ein Gutachter für Drittparteirisiken (TPR) die Anwendungen zusammen verwenden können, um das Lieferantenrisiko zu bewerten.

Der Workflow Supplier Lifecycle Operations und Risikomanagement von Drittparteien .



In diesem Workflow:

1. Der Lieferantenmanager erhält eine Anforderung zum Lieferanten-Onboarding.
2. Der Lieferantenmanager verwendet das Onboarding-Playbook, das einen optimierten und geführten Prozess für das Onboarding von Lieferanten bietet. Weitere Informationen finden Sie unter Using the supplier onboarding playbook to onboard suppliers .
3. Der Lieferantenmanager übermittelt eine Sorgfaltspflicht-Anforderung.

   Die Durchführung der Sorgfaltspflicht ist ein wichtiger Aspekt beim Onboarding eines Lieferanten. Die Bewertung des Lieferantenrisikos wird vom Gutachter für Drittparteirisiken (TPR) durchgeführt. Weitere Informationen finden Sie unter Erste Schritte mit Risikobewertungsintegration für Lieferantenlebenszyklus-Vorgänge.
4. Der TPR-Manager genehmigt die Sorgfaltspflicht-Anforderung.
5. Der Fragebogen zum inhärenten Risiko wird erstellt und dem TPR-Gutachter zugewiesen.
6. Der TPR-Gutachter übermittelt den abgeschlossenen IRQ.
7. Es werden zwei Risikobewertungsfragebögen erstellt und dem Lieferantenkontakt zugewiesen.
8. Der Lieferantenkontakt meldet sich bei Zusammenarbeitsportal für Lieferanten an und füllt die Fragebögen zur Risikobewertung aus.
9. Ein Vertragsdatensatz wird mit einer Genehmigung erstellt. Nachdem der Vertragsdatensatz genehmigt wurde, wird der Risikodatensatz mit der endgültigen Bewertung aktualisiert.
10. Der Lieferantenmanager akzeptiert die Risikoeinstufung und schließt die Sorgfaltspflicht-Anforderung.

Automatische Übersetzung

Anforderungen für die Integration Supplier Lifecycle Operations von und Risikomanagement von Drittparteien

1. Installieren Sie die Anwendung Supplier Lifecycle Operations (com.snc.sn_supplier_mgmt) aus dem ServiceNow® Store. Weitere Informationen finden Sie unter Install Supplier Lifecycle Operations.
2. Installieren und aktivieren Sie das Plugin „Risk Assessments Integration for Supplier Lifecycle Operations“ (com.snc.sn_supplier_tprm).
3. Installieren Sie die Anwendung Risikomanagement von Drittparteien (com.sn_vdr_risk_asmt) aus dem ServiceNow® Store. Weitere Informationen finden Sie unter Configuring Third-party Risk Management.
4. Installieren und aktivieren Sie das Plugin „GRC: Drittpartei-Sorgfaltspflicht-Anforderung“ (com.sn_tprm_onboarding).

Hinweis:
Sie benötigen eine Lizenz für Risikomanagement von Drittparteien (früher Vendor Risk Management), um diese bessere Zusammenarbeitslösung nutzen zu können.

Erste Schritte mit Risikobewertungs-Integration für Supplier Lifecycle Operations

Machen Sie sich mit der Risikobewertungs-Integration für Supplier Lifecycle Operations durch, indem Sie die folgenden Aufgaben ausführen:

1. Erstellen Sie einen Lieferanten. Weitere Informationen finden Sie unter Create a supplier from the Source-to-Pay Workspace.
2. Onboarding eines neuen Lieferanten mithilfe von Playbooks. Weitere Informationen finden Sie unter Using the supplier onboarding playbook to onboard suppliers.
3. Das Playbook erstellt eine Sorgfaltspflicht-Anforderung. Weitere Informationen zu den Feldern in dieser Aktivität finden Sie unter Request due diligence for a third-party engagement.
4. Der Lieferantenmanager füllt eine Sorgfaltspflicht-Anforderung aus und übermittelt sie, die dem TPR-Manager zugewiesen wird.

   Hinweis:
   Für jede Sorgfaltspflicht-Anforderung weist das System automatisch eine eindeutige ID-Nummer zu, die mit dem Präfix **DDR**beginnt.

5. Wenn die Sorgfaltspflicht-Anforderung vom TPR-Manager genehmigt wird, wird der Fragebogen zum inhärenten Risiko an den TPR-Gutachter (internen Stakeholder) gesendet.
6. Nachdem der TPR-Gutachter den abgeschlossenen IRQ übermittelt hat, beginnt der Sorgfaltspflichtprozess.
7. Im Rahmen des Sorgfaltspflicht-Prozesses werden zwei Risikobewertungen erstellt, die jeweils einen Fragebogen zur externen Sorgfaltspflicht enthalten – eine für die Drittpartei und eine für die Interaktion.
8. Nachdem die Lieferantenkontakte die externen Fragebogen aus dem Zusammenarbeitsportal für Lieferanten ausgefüllt und übermittelt haben, geht der TPR-Manager die Fragebogen durch und genehmigt die Sorgfaltspflicht-Anforderung. Weitere Informationen finden Sie unter Complete a risk assessment from the Supplier Collaboration Portal.

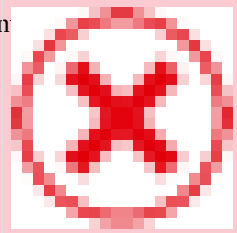
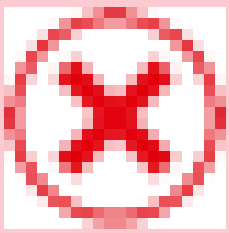
9. Ein Vertragsdatensatz wird mit einer Genehmigung erstellt. Nachdem der Vertragsdatensatz genehmigt wurde, wird der Risikodatensatz mit der endgültigen Bewertung aktualisiert.
10. Nachdem der Lieferantenmanager die Risikobewertung akzeptiert hat, wird eine E-Mail an die anfordernde Person gesendet, in der er informiert wird, dass die Sorgfaltspflicht-Anforderung erfolgreich verarbeitet und genehmigt wurde.
11. Der Lieferantenmanager schließt die Sorgfaltspflicht-Anforderung (den Fall).
12. Als Lieferantenmanager können Sie die Ergebnisdaten der Risikobewertung in Kombination mit anderen Daten verwenden, um zu bestimmen, ob der Onboarding-Prozess fortgesetzt oder abgebrochen werden soll.

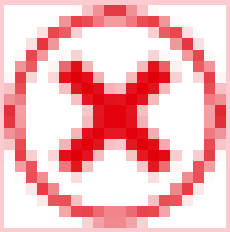
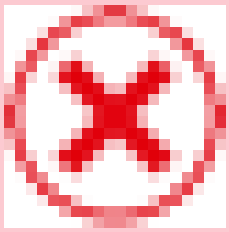
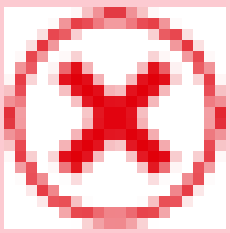
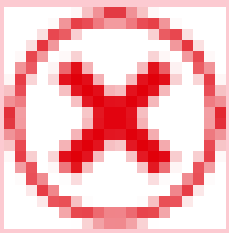
[store-future: BEGIN review]

Reduzieren Sie das Technologierisiko, die technischen Schulden und die Anwendungskosten

Mit Arbeitsbereich Enterprise Architecture, IT Asset Managementund Information Technology Operations ManagementAnwendungsportfolio analysieren, Aktualisierungszyklen verwalten und Legacy-Anwendungen rationalisieren

Kombinationsvorteile der Integration von Arbeitsbereich Enterprise Architecture mit IT Asset Management und IT Operations Management

Funktion	EA-Arbeitsbereich	ITAM	ITOM	Alle Anwendungen zusammen
Konfigurationselemente (CIs) erkennen			 Zum Erkennen des Bestands an Software und Hardware	ITOM Discovery identifiziert und fügt der CMDB Hardware- und Software-Konfigurationselemente hinzu, einschließlich Geschäftsanwendungen und Anwendungsservices. Discovery bietet einen aktuellen Bestand an Software und Hardware. Mit APM erhalten Sie vollständige Einblicke in Ihren Anwendungsbestand.

Funktion	EA-Arbeitsbereich	ITAM	ITOM	Alle Anwendungen zusammen
Service-Mapping			ordnen Sie die Infrastruktur der Business Capability zu.	Service Mapping stellt die Beziehungen zwischen einer Anwendungsinstanz und der erkannten Infrastruktur bereit. Service Mapping erstellt Business Service-Kontextabhängigkeiten für die erkannten CIs, die die Anwendung unterstützen (Anwendungsinstanzen oder Anwendungsservices für Produktions-, Entwicklungs- und Testumgebungen).
Lebenszyklusinhalte von standardisierten Software- und Hardware-Produktmodellen				Software Asset Management (SAM) erstellt einen normalisierten Bestand der Softwaremodelle, die einen Anwendungsservice unterstützen. Das Technologie-Portfoliomanagement (TPM) von APM verwendet den SAM-Softwarebestand, um die Lebenszyklen der Lieferanten zu verwalten. Als Teil von APM nutzt die Funktion „Technologie-Portfoliomanagement“ Daten zum Software- und Hardware-Lebenszyklus von SAM/HAM, um proaktiv zu identifizieren,

Automatische Übersetzung

Funktion	EA-Arbeitsbereich	ITAM	ITOM	Alle Anwendungen zusammen
				welche Geschäftsanwendungen technisch gefährdet sind, da sie von nicht unterstützter oder am Ende der Lebensdauer stehender Software und Hardware abhängig sind.

– APM nutzt diese Funktion, um Transparenz in Bezug auf die mit einer Geschäftsanwendung verbundenen Risiken zu schaffen, z. B. Verlust der Verfügbarkeit und Nachverfolgung der Kontrollen, die zum Testen der Compliance der Anwendung mit Vorschriften angewendet werden. Die kontinuierliche Compliance-Überwachung stellt sicher, dass diese Anwendungen anhand der richtigen Kontrollen zertifiziert werden. Dadurch können wir die organisationale Resilienz von Geschäftsanwendungen sicherstellen. Da die Häufigkeit und der Schweregrad von Angriffen weiter zunehmen, können Unternehmen von der Menge an Sicherheitswarnungen überfordert sein, und es wird schwierig, Bedrohungen schnell zu priorisieren und zu beheben.

Workflow von Arbeitsbereich Enterprise Architecture

Verwenden Sie Arbeitsbereich Enterprise Architecture und IT Asset Management und IT Operations Management zusammen für die folgenden Vorteile:

- Ermöglichen Sie Enterprise Architects, die Nachverfolgung von Versionen und Lebenszyklen der zugrunde liegenden Technologien zu automatisieren und zu bestimmen, welche Geschäftsanwendungen aufgrund abgelaufener oder am Ende der Lebensdauer stehender Technologien gefährdet sind.
- Höhere Transparenz des Anwendungsbestands. Erkennen Sie redundante und veraltete Anwendungen, und treffen Sie entsprechende schnelle Entscheidungen.
- Führen Sie umsetzbare Workflows durch, um zu verhindern, dass für Lizenzen, die nicht mehr verwendet werden, zu viel ausgegeben wird.

Anforderungen für Arbeitsbereich Enterprise Architecture, IT Asset Managementund IT Operations Management

- Installieren Sie die Anwendung Arbeitsbereich Enterprise Architecture (sn_apm_ws).
- Installieren Sie die Anwendung Technologie-Portfoliomanagement (sn_apm_tpm).
- Installieren Sie die Anwendung Software Asset Management Professional (com.sn_samp_master).
- Installieren Sie die Anwendung Hardware Asset Management (com.sn_hamp).

Erste Schritte bei der Bewertung von Technologierisiken für Ihr Unternehmen

Führen Sie die folgenden Schritte aus, um mit der Bewertung von Technologierisiken zu beginnen:

1. Richten Sie die Technologien Ihrer Geschäftsanwendungen an Ihren strategischen Geschäftsinitiativen aus. Sie können eine regelmäßige Aufgabe ausführen, um die Technologie-Lebenszyklusdaten für Ihr Technologieportfolio abzurufen. Weitere Informationen finden Sie unter Run a scheduled job to generate TPM lifecycle data .
2. Zeigen Sie das Risiko des Technologielebenszyklus für Geschäftsanwendungen, Anwendungsservices, Server, Softwareprodukte und Hardwaremodelle auf der Registerkarte **Technologieportfolio** im Abschnitt „Einblicke“ von EA-Arbeitsbereichan. Sie können diese Technologie-Lebenszyklusrisiken filtern, um sie nur für die Anwendung anzuzeigen, an der Sie interessiert sind. Weitere Informationen finden Sie unter Viewing insights of your portfolio .
3. Verfolgen Sie den Fortschritt der Analyse von Technologie-Portfoliomanagement (TPM), indem Sie die Tabelle „Ausführungsprotokoll für erkannte TPM-Technologie“ [sn_apm_tpm_discovered_technologie_run_log] untersuchen. Jedes Mal, wenn die Analyse ausgeführt wird, wird dieser Tabelle ein Eintrag hinzugefügt. Um die Ausführungsprotokolle anzuzeigen, navigieren Sie im EA-Arbeitsbereich zur **Portfolio** -Listenansicht (EA-Arbeitsbereich > Portfolio > Technologie-Portfoliomanagement > Protokolle). Weitere Informationen finden Sie unter Portfolio list view .
4. Rationalisieren Sie Ihre Geschäftsanwendungen, um Geschäftsanwendungen basierend auf mehreren Punktzahlen zu analysieren, einen Bedarf für eine Geschäftsanwendung zu erstellen, die geplante Disposition einer Geschäftsanwendung festzulegen und Lebenszyklusdetails zu einer vorhandenen Geschäftsanwendung hinzuzufügen. Weitere Informationen finden Sie unter Rationalization of business applications .

[End]