servicenow

Zürich Besser Zusammen

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

servicenow

Inhaltsverzeichnis

Automatische Übersetzung

Lösungen

Verbessern Sie mit Lösungen die Funktionalität von ServiceNow Anwendungen, indem sie in Kombination miteinander verwendet werden.

Verfügbare Lösungen

Erfahren Sie mehr über die Vorteile der einzelnen Lösungen und deren Implementierung und Verwendung.

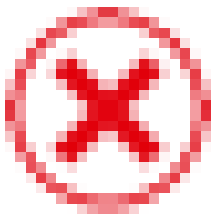
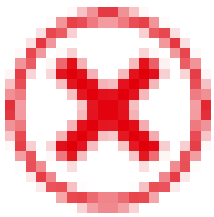
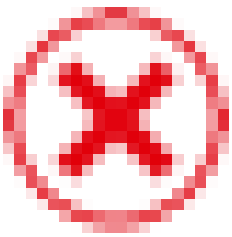
Verbessern Sie die Transparenz des organisatorischen Risikorisikorisikos mit der erweiterten Projektrisikobewertung

Mit der erweiterten Risikobewertung für Ihre Projekte können Sie leicht erkennen, ob Projekte potenzielle Organisationsrisiken darstellen, und schnell über mindernde Aktionen entscheiden. Kombinieren Sie Projekt-Risikomanagement mit Enterprise-Risikomanagement, um einen besseren Einblick in das Gesamtrisikorisiko Ihrer Organisation zu erhalten.

Kombinierte Vorteile der Integration Projekt-Portfoliomanagement Mit Erweitertes Risikomanagement

Funktion	Projekt-Portfoliomanagemen	Erweitertes Risikomanagement	Beide Anwendungen zusammen
Projektrisikobewertung	✓	✗	✓
Erhöhung auf Enterprise-Risiko	✗	✗	✓
Bewertung inhärenter Risiken und Restrisiken	✓	✓	✓
Integrierte Projekt- und Enterprise-Risikoregister	✗	✗	✓

Automatische Übersetzung

Funktion	Projekt-Portfoliomanagemen	Erweitertes Risikomanagement	Beide Anwendungen zusammen
Risiko-Heatmaps			
Dashboard „Risikoübersicht für Enterprise-Projekte“			

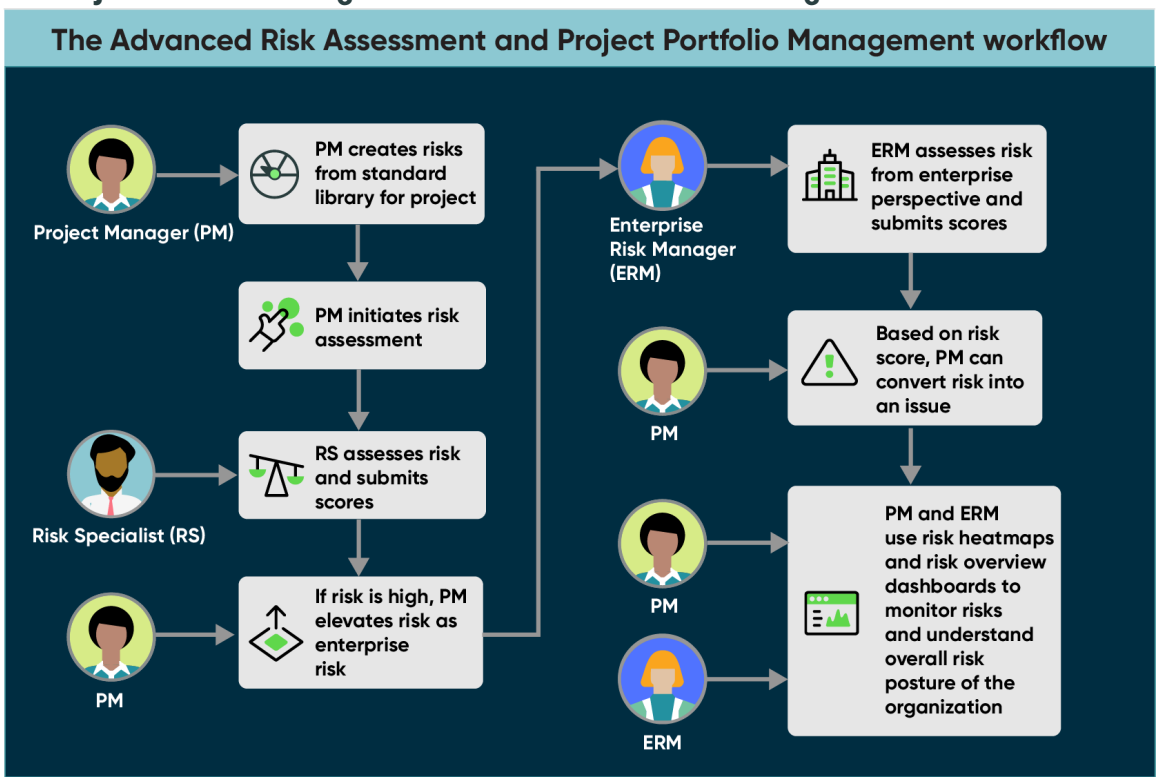
Workflow der erweiterten Projektrisikobewertung

Verwenden Projekt-Portfoliomanagement(PPM) und Erweitertes Risikomanagement Bewertung (ARA) zusammen für diese Vorteile:

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

Die folgende Abbildung zeigt einen Beispiel-Workflow, wie ein Projektmanager, Risikospezialist und Enterprise Risk Manager die Anwendungen gemeinsam verwenden, um Risiken sowohl auf Projekt- als auch auf Unternehmensebene zu bewerten und zu mindern.

Die Projekt-Portfoliomanagement Und Erweitertes Risikomanagement Workflow



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 gibt ihm eine Bewertungspunktzahl.
3. Wenn die Risikopunktzahl hoch ist, erhöht der Projektmanager das Risiko als Unternehmensrisiko.
4. Der Enterprise Risk Manager bewertet das Risiko aus der Unternehmensperspektive und gibt ihm eine Bewertungspunktzahl.
5. Basierend auf der Risikopunktzahl kann der Projektmanager das Risiko in ein Problem konvertieren.
6. Der Projektmanager und der Enterprise Risk Manager verwenden Risiko-Heatmaps und Risikoübersichts-Dashboards, um Risiken zu überwachen und die Gesamtrisikosituation der Organisation zu verstehen.

Anforderungen für Projekt-Portfoliomanagement Und Erweitertes Risikomanagement Integration

1. Aktivieren Sie das Plugin „Projekt-Portfoliomanagement“ [com.snc.Financial_Planning_pmo].
2. Installieren Sie die Anwendung GRC: Advanced Risk aus der ServiceNow® Store.

Erste Schritte mit der erweiterten Projektrisikobewertung

Um mit der Bewertung Ihrer Projektrisiken zu beginnen, führen Sie die folgenden Schritte aus:

1. Richten Sie die Risikobewertungsmethode ein, und konfigurieren Sie sie. Siehe Konfigurieren Sie Projekt-Portfoliomanagement und erweiterte Risikointegration .

   Rolle: sn_Risk.admin.

2. Definieren Sie den Umfang, und initiieren Sie die Risikobewertung. Siehe Fügen Sie Risiken für ein Projekt hinzu .

   Rolle: IT_project_Manager.

3. Führen Sie eine Risikobewertung durch. Siehe Führen Sie eine Risikobewertung durch .

   Rolle: sn_grc.Business_user.

4. Bewerten und erhöhen Sie das Projektrisiko. Siehe Erhöhen Sie ein Projektrisiko auf ein Unternehmensrisiko .

   Rolle: IT_project_Manager.

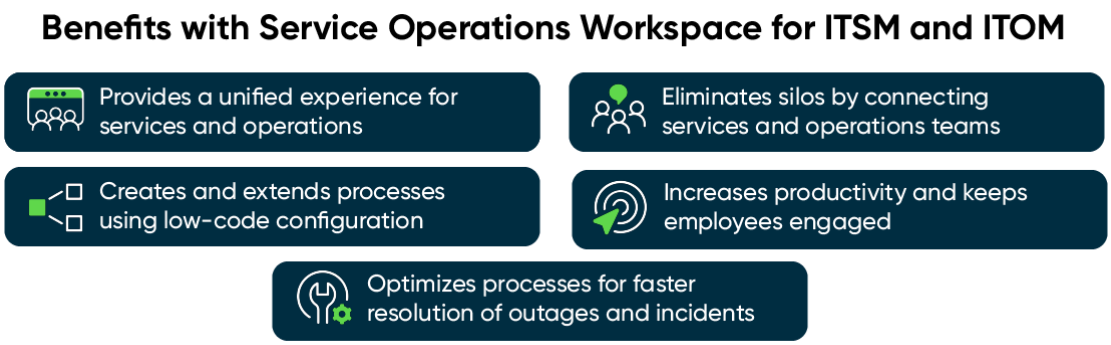
5. Konvertieren Sie das Risiko in ein Problem, und überwachen Sie die Sicherheitslage. Siehe Überwachen Sie die Risikolage .

   Rolle: sn_Risk.admin, IT_Project_Manager.

Automatisieren und Optimieren Ihrer Services und Vorgänge mit Service Operations-Arbeitsbereich

Sie können Services erweitern und gleichzeitig Kosten reduzieren, hochwertige Kunden- und Mitarbeiter-Experiences bereitstellen und die betriebliche Resilienz fördern. Verwenden Sie eine einzige Cloud-Plattform, die IT-Prozesse wie Incident, Problem und Change in IT-Vorgänge wie Discovery, Business-Service-Definitionen, Service-Zuordnung und Ereignismanagement integriert.

Kombinierte Vorteile der Integration Service Operations-Arbeitsbereich Für IT Service Management(ITSM) Und IT Operations Management(ITOM)



Automatische Übersetzung

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

Automatische Übersetzung

Funktion	Service Operations-Arbeitsbereich für ITSM	Service Operations-Arbeitsbereich für ITOM	Alle Anwendungen zusammen
Geführte Experience für die Erstkonfiguration von Service Operations-Arbeitsbereich	✓	✗	✓
Präsentation des vollständigen Kontexts eines Service mit zugehörigen Metriken, Protokollen und zusätzlichen Informationen	✗	✓	✓
Schnelle Korrektur für Warnungen zu einem Service	✗	✓	✓
Schnelle Automatisierung für Bediener bei Verwendung einer eingebetteten Playbook-Experience in den Warnungsformularen	✗	✓	✓

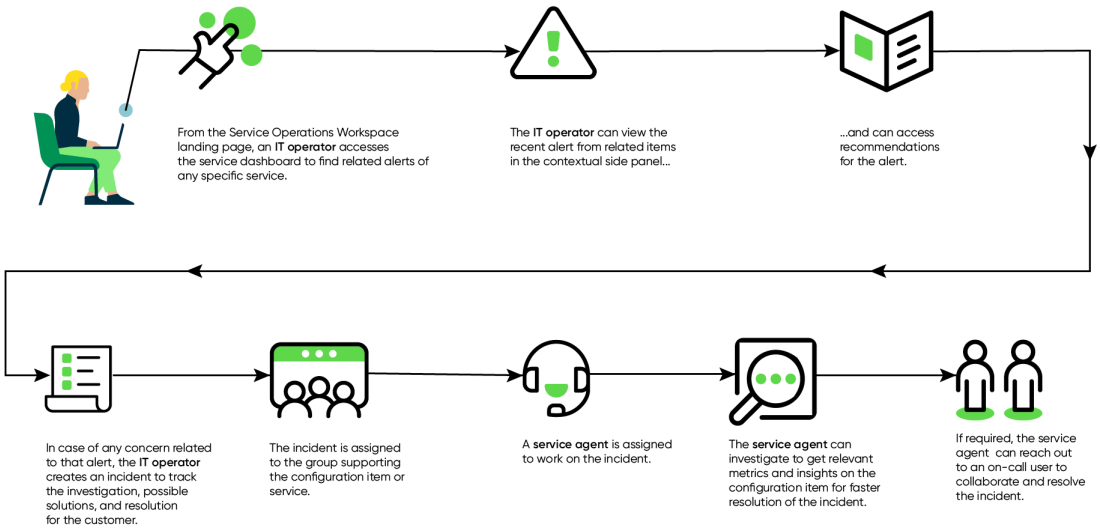
Workflow für Service Operations-Arbeitsbereich

Verwenden Service Operations-Arbeitsbereich Für IT Service Management(ITSM) Und IT Operations Management(ITOM) Zusammen für diese Vorteile:

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

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

Service Operations-Arbeitsbereich Für ITSM Und ITOM Workflow



In diesem Workflow:

1. Von Service Operations-Arbeitsbereich Zielseite, greift ein IT-Betreiber auf das Service-Dashboard zu, um zugehörige Warnungen zu einem bestimmten Service zu finden.
2. Der IT-Betreiber kann die letzte Warnung aus zugehörigen Elementen im kontextbezogenen Seitenbereich anzeigen.
3. Der IT-Betreiber kann auf Empfehlungen für die Warnung zugreifen.
4. Wenn im Zusammenhang mit dieser Warnung ein Kundenproblem auftritt, erstellt der IT-Betreiber einen Incident, um die Untersuchung, mögliche Lösungen und Lösungen für den Kunden nachzuverfolgen.
5. Der Incident wird der Gruppe zugewiesen, die das Konfigurationselement oder den Service unterstützt.
6. Ein Service Desk-Mitarbeiter, z. B. ein Service Desk-Mitarbeiter oder L2/L3-Spezialist, wird der Bearbeitung des Incident zugewiesen.
7. Der Service Desk-Mitarbeiter kann untersuchen, um relevante Metriken und Einblicke in das Konfigurationselement zu erhalten, um den Incident schneller zu lösen.
8. Bei Bedarf kann sich der Service Desk-Mitarbeiter an einen Rufbereitschaftsanwender wenden, um zusammenzuarbeiten und den Incident zu lösen.

Anforderungen für die Integration Service Operations-Arbeitsbereich Für ITSM Und ITOM

1. Stellen Sie sicher, dass die folgenden Bedingungen für erfüllt sind Service Operations-Arbeitsbereich Für ITSM.
   a. Beschaffen Sie sich ITSM Standardlizenz oder höher für ServiceNow® IT Service Management Anwendungen. Wenden Sie sich an Ihren ServiceNow Account-Manager oder Vertriebsmitarbeiter.
   b. Wenn Sie das Untersuchungs-Framework in verwenden möchten Service Operations-Arbeitsbereich Für ITSM, Beschaffen Sie ITSM Berufslizenz oder höher für ServiceNow® IT Service Management Anwendungen.
   c. Installieren Service Operations-Arbeitsbereich ITSM Anwendungen aus dem ServiceNow® Store. Informationen zur Installation dieser Anwendung finden Sie unter Installieren Sie ITSM-Anwendungen für Service Operations-Arbeitsbereich .
2. Stellen Sie sicher, dass die folgenden Bedingungen für erfüllt sind Service Operations-Arbeitsbereich Für ITOM.
   a. Beschaffen Sie sich ITOM Berufslizenz oder höher für ServiceNow® IT Operations Management Anwendungen. Wenden Sie sich an Ihren ServiceNow Account-Manager oder Vertriebsmitarbeiter.
   b. Installieren Service Operations-Arbeitsbereich ITOM Anwendungen aus dem ServiceNow® Store. Informationen zur Installation dieser Anwendung finden Sie unter Installieren Sie Service Operations-Arbeitsbereich für ITOM-Anwendungen .

Erste Schritte mit Service Operations-Arbeitsbereich Für ITSM Und ITOM

Um mit zu beginnen Service Operations-Arbeitsbereich Für ITSM Und ITOM, Führen Sie die folgenden Schritte aus:

1. Konfigurieren Service Operations-Arbeitsbereich Für ITSM.
   a. Einrichten Service Operations-Arbeitsbereich Für ITSM. Siehe Service Operations-Arbeitsbereich für ITSM einrichten .

      Rolle: admin.

   b. Richten Sie das Untersuchungs-Framework ein. Siehe Investigations-Framework im Service Operations-Arbeitsbereich einrichten .

      Rolle: admin.

   c. Konfigurieren Sie das Empfehlungs-Framework für einen Incident. Siehe Konfigurieren des Empfehlungs-Frameworks im Service Operations-Arbeitsbereich für ITSM .

      Rolle: admin.

2. Konfigurieren Service Operations-Arbeitsbereich Für ITOM.
   a. Einrichten Service Operations-Arbeitsbereich Für ITOM. Siehe Service Operations-Arbeitsbereich für ITOM einrichten .

      Rolle: evt_mgmt_Operator.

   b. Konfigurieren Sie Warnungsmetriken. Siehe Konfigurieren Sie Warnungsmetriken .

Rolle: evt_mgmt_Operator.

c. Konfigurieren Sie das Empfehlungs-Framework für eine Warnung. Siehe Konfigurieren des Empfehlungs-Frameworks im Service Operations-Arbeitsbereich für ITOM .

Rolle: evt_mgmt_admin.

d. Konfigurieren Sie Service Operations-Arbeitsbereich Posteingang. Siehe Konfigurieren Sie den Posteingang im Service Operations-Arbeitsbereich für ITOM .

Rolle: evt_mgmt_admin.

e. Anpassen Service Operations-Arbeitsbereich Listen. Siehe Passen Sie Listen im Service Operations-Arbeitsbereich für ITOM an .

Rolle: itil.

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

Der Anwendungsfall zeigt, wie es geht ITOM Die Integration hat das Risiko-, Compliance- und Audit-Management für ein Finanzinstitut optimiert, indem operative Transparenz, Automatisierung und erweiterte Risikobewertungen in Echtzeit bereitgestellt werden.

Kurzbeschreibung des Problems

Ein führendes Finanzinstitut versuchte, seine Risikomanagementprozesse während des Wachstums zu optimieren und dabei zunehmend komplexe Betriebs-, Drittpartei- und Technologierisiken sowie Compliance- und interne Auditfunktionen zu behandeln. Die Institution erkannte die Notwendigkeit einer einheitlichen Plattform, um die Effizienz zu verbessern und den manuellen Aufwand zu reduzieren.

Herausforderungen

- Fehlende zentrale Transparenz: Das Finanzinstitut sah sich mit Herausforderungen konfrontiert, eine klare Echtzeitansicht von Risiken, Compliance und Audit-Prozessen zu erhalten. Unterschiedliche Systeme machten es schwierig, Betriebsrisiken im Zusammenhang mit IT-Services und -Infrastruktur zu bewerten.
- Isolierte IT-Infrastruktur: Die nicht verbundenen IT-Systeme der Institution machten die Überwachung und Reaktion auf betriebliche Probleme schwierig, die sich auf Risikomanagementfunktionen auswirken könnten, z. B. Ausfallzeiten, Konfigurationsfehler und IT-Servicefehler.
- Eingeschränkte Nutzung vorhandener Daten: Die beträchtliche Menge an IT-Daten, die aus verschiedenen Quellen verfügbar sind, wurde aufgrund der fehlenden Integration mit vorhandenen Systemen nicht vollständig für das Risiko- und Compliance-Management genutzt.

ITOM-spezifische Lösungen

- Operative Transparenz in Echtzeit: ITOM Bot der Institution Echtzeiteinblicke in die Integrität, Verfügbarkeit und Leistung von IT-Services. Durch Integration ITOM Mit ServiceNow IRM, Risiko- und Compliance-Teams konnten Betriebsrisiken (z. B. Serviceausfälle, Leistungsverschlechterungen) direkt mit umfassenderen Risikomanagementmaßnahmen korrelieren.

- Automatisiert Service-Mapping Für eine bessere Risikobewertung: Die Service-Mapping Fähigkeiten in ITOM Hat der Institution ermöglicht, IT-Services automatisch zuzuordnen 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 sofort im Compliance-Dashboard als Ereignis mit hohem Risiko kennzeichnen, sodass die Institution Präventivmaßnahmen ergreifen kann.
- Proaktive Überwachung und Warnungsantwort: Durch Nutzung ITOM Ereignismanagement, Die Institution konnte wichtige Betriebsrisiken wie Systemausfälle und Serviceausfälle von Drittparteien überwachen und automatisierte Warnungen an relevante Risikomanagement- und Compliance-Teams auslösen. Dieser proaktive Ansatz hat die Zeit zwischen der Identifizierung eines Betriebsrisikos und der Reaktion darauf minimiert.
- Configuration Management Database (CMDB) Für Compliance: Die Integration von ITOM Mit CMDB Sichergestellt, dass alle IT-Assets, Konfigurationen und ihre Beziehungen genau nachverfolgt wurden. Dies bot eine zentrale Wahrheitsquelle für das Risikomanagement, sodass Compliance-Teams Risiken automatisch mit bestimmten IT-Assets oder -Services verknüpfen können, wodurch genauere Risikobewertungen sichergestellt werden, insbesondere im Kontext von Technologierisiken und Abhängigkeiten von Drittparteien.
- Reduzierung und Automatisierung von Warnungsrauschen: ITOM AIOps wurde genutzt, um die Ermüdung von Warnungen zu reduzieren, indem zugehörige Warnungen (z. B. aufgrund von Infrastrukturfehlern) automatisch gruppiert und korreliert wurden. Dadurch wurde der manuelle Aufwand für Risiko- und Compliance-Teams reduziert, um irrelevante Warnungen zu durchsuchen, sodass sie sich auf Betriebsrisiken mit höherer Priorität konzentrieren können.

Wichtige Ergebnisse

- Einheitlicher Risiko- und IT-Betrieb: Durch Integration ITOM Mit ServiceNow IRM, Die Institution hat eine einheitliche Ansicht sowohl der Betriebs- als auch DER IT-Risiken erreicht. Diese Integration erleichterte die Identifizierung von Risiken, die aus betrieblichen IT-Ausfällen resultieren, und half der Institution, kritische Warnungen schnell zu beheben, bevor sie eskaliert wurden.
- Verbesserte Effizienz durch Automatisierung: ITOM Die Automatisierung half der Institution, manuelle Prozesse im Zusammenhang mit der Überwachung von Betriebsrisiken zu eliminieren, z. B. die manuelle Nachverfolgung von Serviceunterbrechungen oder Änderungen in der IT-Umgebung, die neue Risiken mit sich bringen könnten.
- Verbesserte Compliance mit IT-bezogenen Vorschriften: Die von bereitgestellten Echtzeitdaten ITOM Stellte sicher, dass die Institution regulatorische Anforderungen in Bezug auf IT-Risiken und Audit-Bereitschaft erfüllen konnte. Die Fähigkeit von ITOM Um alle IT-Assets und Konfigurationen auf dem neuesten Stand zu halten, wurden Audit-Prozesse schneller und genauer.
- Skalierbarkeit für zukünftige Risikomanagementanforderungen: Die Cloud-native Architektur von ITOM Bereitstellung von Skalierbarkeit und Flexibilität, um sicherzustellen, dass die Institution Risiken auch weiterhin verwalten konnte, wenn sie wuchs. ITOM Unterstützt wurde auch mobiler Zugriff, der Remote-Überwachung und Warnungsmanagement durch Risiko- und IT-Teams ermöglicht.

Verfolgen Sie die Leistung Ihrer IT-Assets mit nach Hardware Asset Management Und Nachhaltige IT

Die Nachhaltige IT Mit der Anwendung können Sie die von Ihren Hardware-Assets generierten Emissionen effektiv verwalten und überwachen. Darüber hinaus können Sie den Energieverbrauch Ihrer Assets und ihre ordnungsgemäße Entsorgung nachverfolgen, nachdem sie das Ende ihrer Lebensdauer erreicht haben.

Kombinierte Vorteile der Integration Hardware Asset Management Und ESG Management S Nachhaltige IT

Funktion	Hardware Asset Management	ESG Management	Alle Anwendungen zusammen
Hardware-Asset-Bestandsverwaltung	✓	✗	✓
Schätzen Sie den Energieverbrauch und die Emissionen von Hardware-Assets	✗	✓	✓
Lebenszyklus-Nachverfolgung von Hardware-Assets	✓	✗	✓
Melden Sie die Reduzierung von E-Abfall	✗	✓	✓
Erhöhen Sie den Anteil der Energy Star-zertifizierten Assets im Portfolio	✗	✗	✓

Automatische Übersetzung

Funktion	Hardware Asset Management	ESG Management	Alle Anwendungen zusammen
Verfolgen Sie Energieverbrauch, CO2-Emissionen und erneuerbare Energien im Rechenzentrum	✗	✓	✓
Überwachen Sie PUE, WUE und CUE von jedem Standort aus, um gezielte Verbesserungen zu erzielen	✗	✗	✓
Verfolgen Sie alle relevanten Metriken für nachhaltige IT auf einen Blick	✗	✗	✓

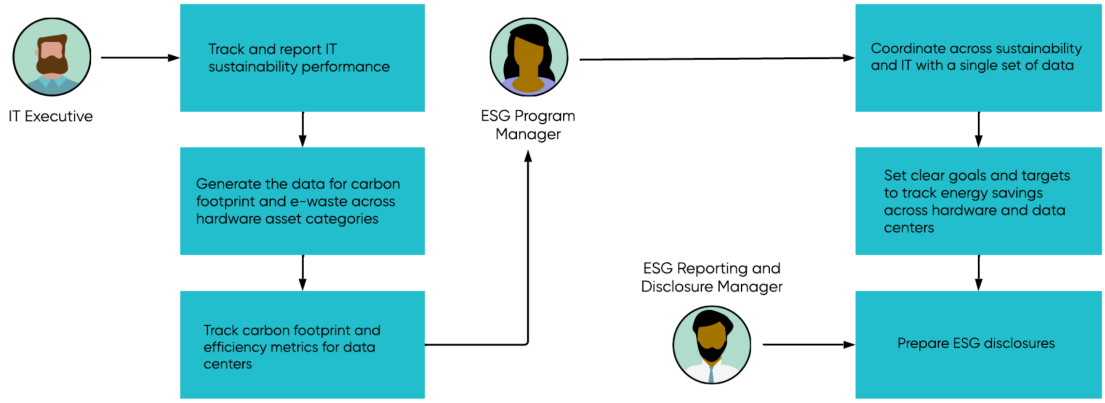
Workflow zur Verwendung Hardware Asset Management Und Nachhaltige IT

Verwenden Hardware Asset Management Und Nachhaltige IT Anwendungen zusammen bieten die folgenden Vorteile:

- Ermöglicht es Ihnen, die von Ihren Hardware-Assets generierten Emissionen effektiv zu verwalten und zu überwachen
- Hilft Ihnen, den Energieverbrauch Ihrer Assets und ihre ordnungsgemäße Entsorgung nach dem Ende ihrer Lebensdauer nachzuverfolgen.
- Bietet wertvolle Einblicke über ein Dashboard, mit dem Sie fundierte Entscheidungen darüber treffen können, ob diese Assets stillgelegt oder wiederverwendet werden sollen

Die Abbildung zeigt die Zusammenarbeit zwischen einem IT-Mitarbeiter und dem Nachhaltigkeitsprogramm-Manager bei der Erfassung von Daten zum CO2-Fußabdruck und E-Abfall. Die ESG-Programmmanager legen Ziele und Ziele fest, um die Wirksamkeit von Energiesparmaßnahmen zu überwachen und Offenlegungen vorzubereiten.

Die Hardware Asset Management Und Nachhaltige IT Workflow



In diesem Workflow:

1. Der IT-Manager meldet sich beim Asset Executive Workspace an, um die Leistung der IT-Nachhaltigkeit nachzuverfolgen und zu melden.
2. Der IT-Manager erhält dann den CO2-Fußabdruck und den E-Abfall, der in verschiedenen Hardware-Asset-Kategorien generiert wurde, und verfolgt die CO2-Fußabdruck- und Effizienzmetriken für Rechenzentren.
3. Der ESG-Programmmanager koordiniert mit einem einzigen gemeinsam genutzten Datensatz zwischen Nachhaltigkeit und IT.
4. Die ESG-Programmmanager legen Ziele und Ziele fest, um die Wirksamkeit von Energiesparmaßnahmen zu überwachen und so dem ESG-Reporting- und Offenlegungsmanager bei der Vorbereitung von Offenlegungen zu helfen.
5. Der ESG-Berichterstellungs- und Offenlegungsmanager bereitet die ESG-Offenlegungen vor.

Anforderungen für die Integration Hardware Asset Management Und ESG Management

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

Erste Schritte mit Nachhaltige IT Um Ihre Emissionsdaten aus Ihren IT-Assets nachzuverfolgen

Erste Schritte mit Nachhaltige IT Durch Abschluss dieser Aufgaben:

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 Risikobewertungsintegration für Supplier Lifecycle Operations, Sie können potenzielle Lieferantenrisiken beim Onboarding neuer Lieferanten identifizieren und bewerten.

Kombinierte Vorteile der Integration Supplier Lifecycle Operations Mit Risikomanagement von Drittparteien

Funktion	Supplier Lifecycle Operations	Risikomanagement von Drittparteien	Alle Anwendungen zusammen
Lieferanten-Onboarding	✓	✗	✓
Informations- und Datenverwaltung	✓	✗	✓
Fall- und Konfliktmanagement	✓	✗	✓
Risiko-Onboarding	✗	✓	✓
Drittpartei-Risiko-Sorgfaltspflicht, externe und interne Risikobewertung	✗	✓	✓

Automatische Übersetzung

Funktion	Supplier Lifecycle Operations	Risikomanagement von Drittparteien	Alle Anwendungen zusammen
Risk Intelligence	✗	✓	✓
Risikobewertung und -Überwachung	✗	✓	✓
Dashboard „Risiko-Führungskräfte“	✗	✓	✓

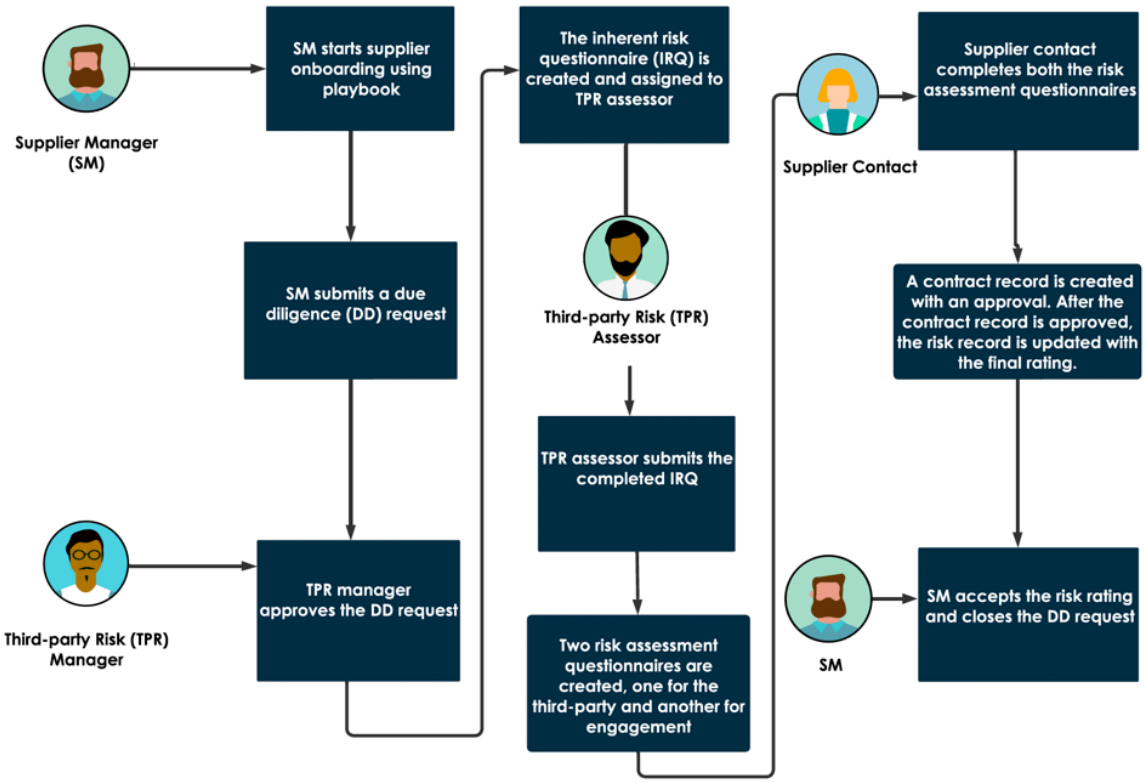
Workflow der Risikobewertungsintegration für Supplier Lifecycle Operations

Verwenden Supplier Lifecycle Operations Und Risikomanagement von Drittparteien Gemeinsam für diese Vorteile:

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

Die folgende Abbildung zeigt einen Beispiel-Workflow, wie ein Lieferantenmanager und ein Drittpartei-Risikobewerter die Anwendungen gemeinsam verwenden können, um das Lieferantenrisiko zu bewerten.

Die Supplier Lifecycle Operations Und Risikomanagement von Drittparteien Workflow



In diesem Workflow:

1. Der Lieferantenmanager erhält eine Lieferanten-Onboarding-Anforderung.
2. Der Lieferantenmanager verwendet das Onboarding-Playbook, das einen optimierten und geführten Prozess zum Onboarding von Lieferanten bietet. Weitere Informationen finden Sie unter Use 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 Lieferantenrisikobewertung wird vom Drittpartei-Risikobewerter (TPR) durchgeführt. Weitere Informationen finden Sie unter Erste Schritte mit der Integration von Risikobewertungen für Supplier Lifecycle Operations .
4. Der TPR-Manager genehmigt die Sorgfaltspflicht-Anforderung.
5. Der Fragebogen für inhärentes Risiko wird erstellt und dem TPR-Beurteiler zugewiesen.
6. Der TPR-Beurteiler übermittelt die abgeschlossene IRQ.
7. Zwei Risikobewertungsfragebogen werden erstellt und dem Lieferantenkontakt zugewiesen.
8. Der Lieferantenkontakt meldet sich bei an Zusammenarbeitsportal für Lieferanten Und füllt die Risikobewertungsfragebogen 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 Risikobewertung und schließt die Sorgfaltspflicht-Anforderung.

Anforderungen für die Integration Supplier Lifecycle Operations Und Risikomanagement von Drittparteien

1. Installieren Sie Supplier Lifecycle Operations(Com.snc.sn_Supplier_mgmt) Anwendung aus dem ServiceNow® Store. Weitere Informationen finden Sie unter Install Supplier Case Management .
2. Installieren und aktivieren Sie das Plugin „Risikobewertungsintegration für Supplier Lifecycle Operations“ (com.snc.sn_Supplier_tprm).
3. Installieren Sie Risikomanagement von Drittparteien(Com.sn_vdr_Risk_asmt) Anwendung aus dem ServiceNow® Store. Weitere Informationen finden Sie unter Configuring Third-party Risk Management .
4. Installieren und aktivieren Sie das Plugin GRC: Third-Party Due Diligence Request (com.sn_tprm_Onboarding).

Hinweis:
Sie müssen über eine Lizenz für verfügen Risikomanagement von Drittparteien(Ehemals Vendor Risk Management), um diese bessere Zusammenarbeit-Lösung zu nutzen.

Erste Schritte mit der Integration von Risikobewertungen für Supplier Lifecycle Operations

Erste Schritte mit der Integration von Risikobewertungen für Supplier Lifecycle Operations Durch Abschluss dieser Aufgaben:

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 Use 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 ist.

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

5. Wenn die Sorgfaltspflicht-Anforderung vom TPR-Manager genehmigt wird, wird der Fragebogen zu inhärenten Risiken (IRQ) an den TPR-Beurteiler (interner Stakeholder) gesendet.
6. Nachdem der TPR-Beurteiler die abgeschlossene IRQ übermittelt hat, beginnt der Sorgfaltspflicht-Prozess.
7. Der Sorgfaltspflicht-Prozess erstellt zwei Risikobewertungen, die jeweils einen externen Fragebogen zur Sorgfaltspflicht enthalten, eine für die Drittpartei und eine andere für die Interaktion.
8. Nachdem die Lieferantenkontakte die externen Fragebogen aus dem Portal für Lieferantenzusammenarbeit ausgefüllt und übermittelt haben, durchläuft der TPR-Manager die Fragebogen und genehmigt die Sorgfaltspflicht-Anforderung. Weitere Informationen finden Sie unter Complete a risk assessment from the Supplier Collaboration Portal .

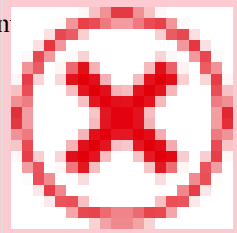
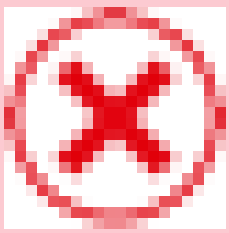
9. Ein Vertragsdatensatz wird mit einer Genehmigung erstellt. Nachdem der Vertragsdatensatz genehmigt wurde, wird der Risikodatensatz mit der endgültigen Bewertung aktualisiert.
10. Nachdem der Lieferantenmanager die Risikobewertung akzeptiert hat, wird eine E-Mail an die anfordernde Person gesendet, die darüber informiert, dass die Sorgfaltspflicht-Anforderung erfolgreich verarbeitet und genehmigt wurde.
11. Der Lieferantenmanager schließt die Sorgfaltspflicht-Anforderung (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]

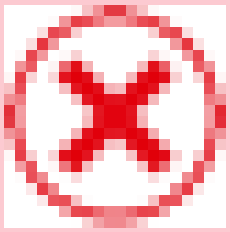
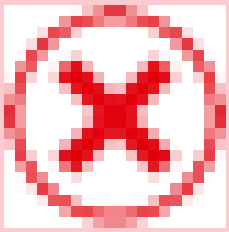
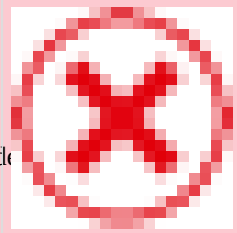
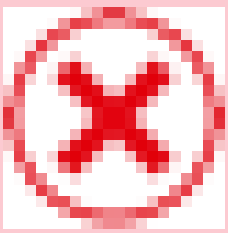
Reduzieren Sie Technologierisiko, technische Schulden und Anwendungskosten

Analysieren Sie das Anwendungsportfolio, verwalten Sie Aktualisierungszyklen, und rationalisieren Sie Legacy-Anwendungen mit Arbeitsbereich Enterprise Architecture, IT Asset Management, Und Information Technology Operations Management

Kombinierte Vorteile der Integration Arbeitsbereich Enterprise Architecture Mit IT Asset Management Und IT Operations Management

Funktion	EA-Arbeitsbereich	ITAM	ITOM	Alle Anwendungen zusammen
Konfigurationselemente (CIs) erkennen			 Erkennen Sie den Bestand an Software und Hardware	Die ITOM-Discovery identifiziert Hardware- und Softwarekonfigurationselemente, einschließlich Geschäftsanwendungen und Anwendungsservices, und fügt sie der CMDB hinzu. Discovery bietet einen aktuellen Bestand an Software und Hardware. Mit APM erhalten Sie vollständigen Einblick in Ihren Anwendungsbestand.

Automatische Übersetzung

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 von den erkannten CIs, die die Anwendung unterstützen (Anwendungsinstanzen oder Anwendungsservices für Produktions-, Entwicklungs- und Testumgebungen).
Standardisierte Inhalte des Lebenszyklus von Software- und Hardwareproduktmode				Software Asset Management (SAM) erstellt einen normalisierten Bestand der Softwaremodelle, die einen Anwendungsservice unterstützen. Das Technology Portolio Management (TPM) von APMs verwendet SAM-Softwarebestand, um die Lebenszyklen des Lieferanten zu verwalten. Als Teil von APM verwendet die Funktionalität „Technologie-Portfoliomanagement“ Software- und Hardware-Lebenszyklusdaten aus SAM/HAM, um proaktiv zu identifizieren, welche

Automatische Übersetzung

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

– APM nutzt diese Fähigkeit, um Einblick in die mit einer Geschäftsanwendung verbundenen Risiken zu bieten, z. B. Verlust der Verfügbarkeit und die Nachverfolgung der Kontrollen, die zum Testen der Compliance von Anwendungen mit Vorschriften angewendet werden. – Die kontinuierliche Compliance-Überwachung stellt sicher, dass diese Anwendungen anhand der richtigen Kontrollen nachgewiesen werden. Somit können wir die operative Resilienz von Geschäftsanwendungen sicherstellen. – Da die Häufigkeit und der Schweregrad des Angriffs weiter zunehmen, können Unternehmen von der Menge der Sicherheitswarnungen überfordert sein und es schwierig finden, Bedrohungen schnell zu priorisieren und zu lösen.

Workflow von Arbeitsbereich Enterprise Architecture

Verwenden Sie Arbeitsbereich Enterprise Architecture Und IT Asset Management Und IT Operations Management Gemeinsam für diese Vorteile:

- Ermöglichen Sie Enterprise Architects, die Nachverfolgungsversionen und Lebenszyklen der zugrunde liegenden Technologien zu automatisieren und zu bestimmen, welche Geschäftsanwendungen aufgrund abgelaufener Technologien oder des Endes ihrer Lebensdauer gefährdet sind.
- Erhöhte Transparenz des Anwendungsbestands. Finden Sie redundante und veraltete Anwendungen heraus, und treffen Sie entsprechende schnelle Entscheidungen.
- Führen Sie umsetzbare Workflows aus, um zu hohe Ausgaben für Lizenzen zu vermeiden, die nicht mehr verwendet werden.

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

- Installieren Sie Arbeitsbereich Enterprise Architecture(sn_apm_WS) Anwendung.
- Installieren Sie Technologie-Portfoliomanagement(sn_apm_tpm) Anwendung.
- Installieren Sie Software Asset Management Professional(Com.sn_samp_Master) Anwendung.
- Installieren Sie Hardware Asset Management(Com.sn_hamp) Anwendung.

Erste Schritte mit der Bewertung von Technologierisiken für Ihr Unternehmen

Um mit der Bewertung Ihrer Technologierisiken zu beginnen, führen Sie die folgenden Schritte aus:

1. Richten Sie die Technologien Ihrer Geschäftsanwendungen an Ihren strategischen Geschäftsinitiativen aus. Sie können eine geplante Aufgabe ausführen, um die Technologie-Lebenszyklusdaten für Ihr Technologieportfolio abzurufen. Weitere Informationen finden Sie unter Run a scheduled job to generate TPM lifecycle data - Legacy .
2. Zeigen Sie das Technologie-Lebenszyklusrisiko für Geschäftsanwendungen, Anwendungsservices, Server, Softwareprodukte und Hardwaremodelle in an **Technologieportfolio** Registerkarte im Abschnitt „Einblicke“ von EA-Arbeitsbereich. 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 von Technologie-Portfoliomanagement(TPM)-Analyse durch Untersuchung der Tabelle „TPM erkanntes Technologieausführungsprotokoll“ [sn_apm_tpm_discovered_Technology_Run_log]. Jedes Mal, wenn die Analyse ausgeführt wird, wird dieser Tabelle ein Eintrag hinzugefügt. Um die Ausführungsprotokolle anzuzeigen, navigieren Sie im EA-Arbeitsbereich zu **Portfolio** Listenansicht (EA-Arbeitsbereich > Portfolio > Technologie-Portfoliomanagement > Protokolle). Weitere Informationen finden Sie unter Exploring 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 einer vorhandenen Geschäftsanwendung Lebenszyklusdetails hinzuzufügen. Weitere Informationen finden Sie unter Rationalization of business applications .

[End]