



# チューリッヒのより良い統合

最終更新日: 2025年12月17日

自動翻訳

これらの資料は、翻訳ソフトウェアを使用してお客様の便宜のために翻訳されています。正確な翻訳をご提供できるよう相当な努力を払っておりますが、いかなる自動翻訳も人間の翻訳者に代わることはなく、そのようなことは意図されておりません。翻訳は「現状のまま」提供されています。他言語への翻訳の的確性、信頼性または正確性については、明示または黙示を問わず、いかなる保証も行われません。翻訳ソフトには限界があるため、一部のコンテンツが正確に翻訳されていない場合があります。これらの資料の公用言語は英語です。翻訳の際に生じる相違または不一致は、コンプライアンスまたは履行の目的に関しては拘束力を有さず、法的効力はないものとします。

ここで示したいくつかの例と図は、説明の目的でのみ提供されています。ServiceNow 製品またはサービスへの実際の関連付けやつながりは意図されておらず、推測されるものではありません。

ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは米国および/またはその他の国における ServiceNow, Inc. の商標または登録商標です。その他の会社名および製品名は、それぞれの所有者の商標です。

下記の ServiceNow ウェブサイト利用規約をお読みください。 [www.servicenow.com/terms-of-use.html](http://www.servicenow.com/terms-of-use.html)

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

# 目次

ソリューション.....	4
高度なプロジェクトリスクアセスメントにより、組織のリスクエクスポージャーの可視化を向上.....	4
を使用したサービスと運用の自動化と最適化 サービスオペレーションワークスペース.....	7
ケーススタディ: リスク、コンプライアンス、 監査管理 の強化 ITOM.....	12
ハードウェア資産管理と持続可能な IT.....	13
オンボーディングプロセス中にサプライヤーを評価することでリスクを最小限に抑える.....	16
技術リスク、技術的負債、およびアプリケーションコストの削減.....	20
[store-future: BEGIN review]	
[End]	

# ソリューション

ソリューションでは、ServiceNow アプリケーションを相互に組み合わせて使用することで、アプリケーションの機能を強化します。

## 利用可能なソリューション


各ソリューションの利点と、その実装方法および使用方法の詳細について説明します。

## 高度なプロジェクトリスクアセスメントにより、組織のリスクエクスポージャーの可視化を向上

プロジェクトの高度なリスクアセスメントを使用すると、潜在的な組織的リスクをもたらすプロジェクトがあるかどうかを簡単に特定し、軽減措置を迅速に決定できます。プロジェクトリスク管理とエンタープライズリスク管理を組み合わせることで、組織の全体的なリスクエクスポージャーの可視化が向上します。

### プロジェクトポートフォリオ管理を統合することの複合的なメリット 高度なリスク

機能	プロジェクトポートフォリオ管理	高度なリスク	両方のアプリケーションをまとめる
プロジェクトリスクアセスメント	✓	✗	✓
エンタープライズリスクへの昇格	✗	✗	✓
固有リスクと残存リスクの評価	✓	✓	✓
統合されたプロジェクトおよびエンタープライズリスク登録	✗	✗	✓
リスクヒートマップ	✗	✓	✓

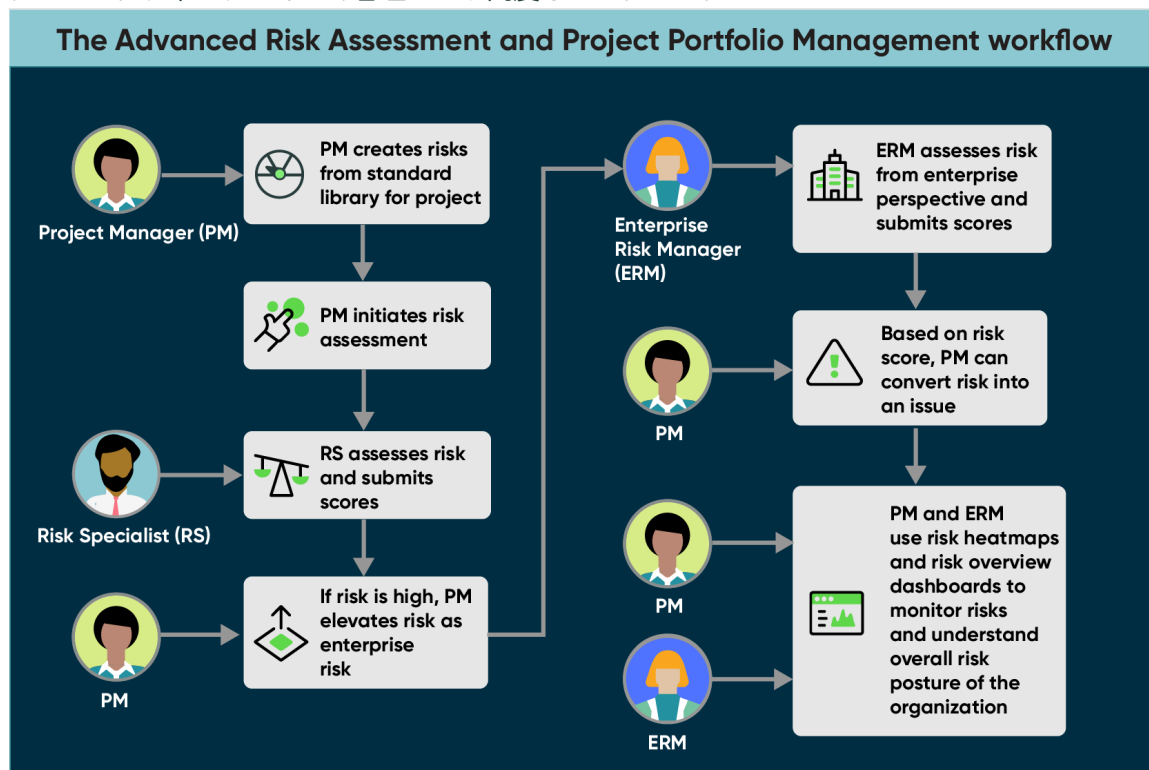
機能	プロジェクトポートフォリオ管理	高度なリスク	両方のアプリケーションをまとめる
エンタープライズプロジェクトリスク概要ダッシュボード			

### 高度なプロジェクトリスクアセスメントのワークフロー

プロジェクトポートフォリオ管理 (PPM) と高度なリスクアセスメント (ARA) を併用すると、次のメリットが得られます。

- 組織レベルでリスクエクスポージャーを監視する
- プロジェクトとエンタープライズの両方のリスクチームのリスク管理システムを統合します。

次の図は、プロジェクトマネージャー、リスクスペシャリスト、およびエンタープライズリスクマネージャーがアプリケーションを組み合わせ使用し、プロジェクトレベルとエンタープライズレベルの両方でリスクを評価して軽減する方法のワークフロー例を示しています。



このワークフローの場合：

1. プロジェクトマネージャーは、プロジェクトの標準ライブラリからリスクを作成し、リスクアセスメントを開始します。
2. リスクスペシャリストがリスクを評価し、アセスメントスコアを付与します。
3. リスクスコアが高い場合、プロジェクトマネージャーはリスクをエンタープライズリスクとして昇格させます。
4. エンタープライズリスクマネージャーは、エンタープライズの観点からリスクを評価し、アセスメントスコアを付与します。
5. リスクスコアに基づいて、プロジェクトマネージャーはリスクを問題に変換できます。
6. プロジェクトマネージャーとエンタープライズリスクマネージャーは、リスクヒートマップとリスク概要ダッシュボードを使用してリスクを監視し、組織の全体的なリスク体制を把握します。

### プロジェクトポートフォリオ管理と高度なリスクの統合の要件

1. プロジェクトポートフォリオ管理プラグイン [com.snc.financial\_planning\_pmo] を有効にします。
2. ServiceNow Storeから GRC:高度なリスクアプリケーションをインストールします。

### 高度なプロジェクトリスクアセスメントの開始

プロジェクトリスクの評価を開始するには、次の手順に従います。

1. リスクアセスメント方法論をセットアップして構成します。「プロジェクトポートフォリオ管理と高度なリスク統合の構成」を参照してください。

ロール:sn\_risk.admin。

2. スコープを定義し、リスクアセスメントを開始します。「プロジェクトのリスクの追加」を参照してください。

ロール:it\_project\_manager。

3. リスクアセスメントを実行します。「リスクアセスメントの実行」を参照してください。

ロール:sn\_grc.business\_user

4. プロジェクトリスクを評価して昇格させます。「プロジェクトリスクをエンタープライズリスクに昇格させる」を参照してください。

ロール:it\_project\_manager。

5. リスクを問題に変換し、セキュリティ体制を監視します。リスク体制の監視を参照してください。

ロール:sn\_risk.admin、 it\_project\_manager。

## を使用したサービスと運用の自動化と最適化 サービスオペレーションワークスペース

コストを削減し、高品質のカスタマーエクスペリエンスと従業員エクスペリエンスを提供し、運用のレジリエンスを促進しながら、サービスを拡張することができます。インシデント、問題、変更などの IT プロセスを、検出、ビジネスサービス定義、サービスマッピング、イベント管理などの IT 運用と統合する単一のクラウドプラットフォームを使用します。

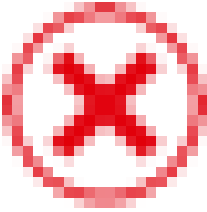


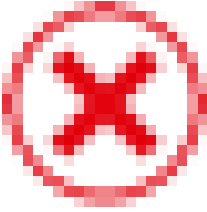


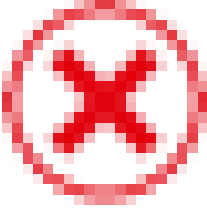


### IT Service Management (ITSM) と IT Operations Management (ITOM) (ITOM) のサービスオペレーションワークスペースを統合することの複合的なメリット

#### 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

機能	ITSM のサービスオペレーションワークスペース	ITOM のサービスオペレーションワークスペース	すべてのアプリケーションをまとめる
シンプルで直感的で明瞭なユーザーインターフェイス (UI)	✓	✓	✓

機能	ITSMのサービスオペレーションワークスペース	ITOMのサービスオペレーションワークスペース	すべてのアプリケーションをまとめる
ユーザーアクションに基づく自動推奨事項	✓	✓	✓
タスクの概要を表示するカスタマイズされたランディングページ	✓	✓	✓
サービスデスクエージェント向けの効果的なインシデント管理	✓	✗	✓
優先度の高いタスクを担当するエキスパート	✓	✗	✓
ログインユーザーのオンボーディングエクスペリエンス	✓	✓	✓
ウォークアップエクスペリエンス	✓	✗	✓
インシデントとインタラクションからの要求管理	✓	✗	✓
の初期構成のガイド付きエクスペリエンス サービスオペレーションワークスペース	✓	✗	✓

機能	ITSMのサービスオペレーションワークスペース	ITOMのサービスオペレーションワークスペース	すべてのアプリケーションをまとめる
関連するメトリクス、ログ、および追加情報を含む、サービスの完全なコンテキストのプレゼンテーション			
サービスのアラートの迅速な修正			
アラートフォーム内で埋め込みプレイブックエクスペリエンスを使用する場合のオペレーターの迅速な自動化			

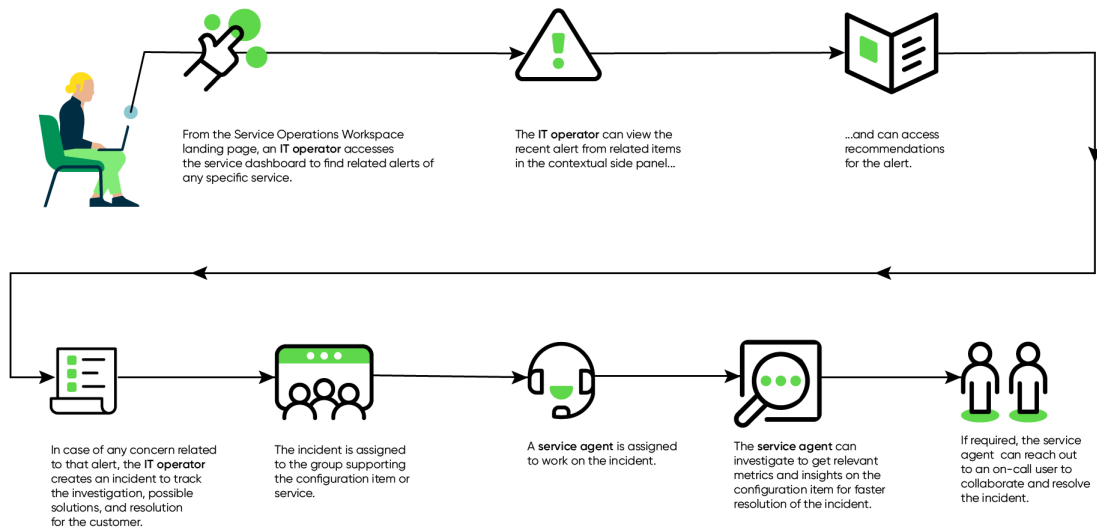
### サービスオペレーションワークスペースのワークフロー

サービスオペレーションワークスペース for IT Service Management (ITSM) とIT Operations Management (ITOM) (ITOM) を併用すると、次のメリットが得られます。

- 単一のプラットフォーム上でサービスと運用に統一されたエクスペリエンスを提供します。
- サービスチームと運用チームをつなぐことでサイロ化を排除します。
- 生産性を向上させ、従業員のエンゲージメントを維持します。
- ローコード構成で ITSM および ITOM プロセスを作成および拡張します。
- インシデントと機能停止を迅速に解決するために、ITSM プロセスと ITOM プロセスを最適化します。

次の図は、IT オペレーターとサービスエージェント (サービスデスクエージェントまたは L2/L3 スペシャリスト) がこれらのアプリケーションを使用して顧客の問題を解決する方法のワークフロー例を示しています。

サービスオペレーションワークスペースの ITSM および ITOM ワークフロー



このワークフローの場合：

1. IT オペレーターは、サービスオペレーションワークスペース ランディングページからサービスダッシュボードにアクセスして、特定のサービスの関連アラートを検索します。
2. IT オペレーターは、コンテキストサイドパネルで関連アイテムから最新のアラートを表示できます。
3. IT オペレーターは、アラートの推奨事項にアクセスできます。
4. そのアラートに関連する顧客の問題がある場合、IT オペレーターはインシデントを作成して、顧客のために調査、可能なソリューション、および解決策を追跡します。
5. インシデントは、構成アイテムまたはサービスをサポートするグループにアサインされます。
6. インシデントの作業を担当するサービスデスクエージェントや L2/L3 スペシャリストなどのサービスエージェントがアサインされます。
7. サービスエージェントは、インシデントを迅速に解決するために、構成アイテム (CI) に関連するメトリクスとインサイトを調査して取得できます。
8. 必要に応じて、サービスエージェントはオンコールユーザーに連絡してコラボレーションを行い、インシデントを解決することができます。

## ITSMとサービスオペレーションワークスペースを統合するための要件ITOM

1. サービスオペレーションワークスペース for ITSM について、次の条件が満たされていることを確認します。
  - a. ServiceNow IT Service Managementアプリケーション用の ITSM Standard ライセンス以降を調達します。ServiceNowアカウントマネージャーまたは営業担当者にお問い合わせください。
  - b. 調査フレームワークを ITSM 用 サービスオペレーションワークスペース 内で使用する場合は、ServiceNow IT Service Management アプリケーション用の ITSM Professional 以降のライセンスを調達します。
  - c. ServiceNow Storeからサービスオペレーションワークスペース ITSMアプリケーションをインストールします。このアプリケーションのインストールの詳細については、「[サービスオペレーションワークスペース ITSM アプリケーションのインストール](#)」を参照してください。
2. サービスオペレーションワークスペース for ITOM について、次の条件が満たされていることを確認します。
  - a. ServiceNow IT Operations Management (ITOM) アプリケーション用の ITOM Professional 以降のライセンスを調達します。ServiceNowアカウントマネージャーまたは営業担当者にお問い合わせください。
  - b. ServiceNow Storeからサービスオペレーションワークスペース ITOMアプリケーションをインストールします。このアプリケーションのインストールの詳細については、「[ITOM アプリケーションのサービスオペレーションワークスペースのインストール](#)」を参照してください。

## ITSM と サービスオペレーションワークスペース の使用を開始するITOM

ITSMおよびITOMのサービスオペレーションワークスペースを開始するには、次の手順に従います。

1. ITSMのサービスオペレーションワークスペースを構成します。
  - a. ITSMのサービスオペレーションワークスペースを設定します。「[ITSM のサービスオペレーションワークスペースの設定](#)」を参照してください。  
 ロール：admin。
  - b. 調査フレームワークを設定します。「[サービスオペレーションワークスペースでの調査フレームワークの設定](#)」を参照してください。  
 ロール：admin。
  - c. インシデントの推奨フレームワークを構成します。「[ITSM のサービスオペレーションワークスペースでの推奨フレームワークの構成](#)」を参照してください。  
 ロール：admin。
2. ITOMのサービスオペレーションワークスペースを構成します。
  - a. ITOMのサービスオペレーションワークスペースを設定します。「[ITOM のサービスオペレーションワークスペースの設定](#)」を参照してください。  
 ロール:evt\_mgmt\_operator。
  - b. アラートメトリクスを設定します。「[アラートメトリクスの設定](#)」を参照してください。  
 ロール:evt\_mgmt\_operator。
  - c. アラートの推奨フレームワークを構成します。「[ITOM のサービスオペレーションワークスペースでの推奨フレームワークの構成](#)」を参照してください。

ルール:evt\_mgmt\_admin。

- d. サービスオペレーションワークスペース受信ボックスを設定します。「ITOM のサービスオペレーションワークスペースでの受信ボックスの構成」を参照してください。

ルール:evt\_mgmt\_admin。

- e. サービスオペレーションワークスペースリストをカスタマイズします。「ITOM のサービスオペレーションワークスペースのリストのカスタマイズ」を参照してください。

ルール:itil。

## ケーススタディ:リスク、コンプライアンス、監査管理の強化 ITOM

このユースケースでは、ITOM 統合によって、リアルタイムの運用の可視化、自動化、および強化されたリスクアセスメントにより、金融機関のリスク、コンプライアンス、および監査管理がどのように合理化されたかを示します。

### 問題の説明

ある大手金融機関は、コンプライアンスおよび内部監査機能に加えて、ますます複雑化する運用、サードパーティ、およびテクノロジーのリスクを処理し、成長に合わせてリスク管理プロセスの合理化を模索していました。この機関は、効率を向上させ、手作業を減らすための統一されたプラットフォームの必要性を認識していました。

### 課題

- 一元化された可視性の欠如:金融機関は、リスク、コンプライアンス、および監査プロセスを明確かつリアルタイムに把握するという課題に直面していました。異種システムでは、IT サービスやインフラストラクチャに関連するオペレーショナルリスクを評価することが困難でした。
- サイロ化された IT インフラストラクチャ:組織の IT システムが分断されていたため、ダウンタイム、構成エラー、IT サービスの障害など、リスク管理機能に影響を与える可能性のある運用上の問題を監視して対応することが困難でした。
- 既存データの限定的な使用:さまざまなソースから利用可能な大量のITデータは、既存のシステムとの統合が行われていないため、リスクおよびコンプライアンス管理に十分に活用されていませんでした。

### ITOM 固有のソリューション

- リアルタイムの運用の可視化: ITOM により、IT サービスの健全性、可用性、およびパフォーマンスに関するリアルタイムのインサイトが機関に提供されました。ITOM ServiceNow IRMと統合することで、リスクチームとコンプライアンスチームは、運用上のリスク(サービス停止、パフォーマンスの低下など)をより広範なリスク管理の取り組みと直接関連付けることができました。
- リスクアセスメントを改善するための自動サービスマッピング:ITOMのサービスマッピング機能により、機関は IT サービスを自動的にマッピングし、その依存関係を理解することができました。これは、オペレーショナルリスクをリアルタイムで評価するために不可欠でした。たとえば、システムが重大なサービス障害を検出し、コンプライアンスダッシュボードで高リスクイベントとして即座にフラグを立てることで、機関が先制的な措置を講じることができます。
- プロアクティブな監視とアラート対応: ITOM イベント管理を活用することで、システム障害やサードパーティのサービス停止などの主要なオペレーショナルリスクを監視し、関連するリスク管理チームとコンプライアンスチームに対して自動アラートをトリガーすることができました。このプロアクティブなアプローチにより、オペレーショナルリスクの特定から対応までの時間が最小限に抑えられました。

- 構成管理データベース (CMDB) コンプライアンス向け: ITOM を CMDB と統合することで、すべての IT 資産、構成、およびそれらの関係が正確に追跡されました。これにより、リスク管理に信頼できる唯一の情報源が提供され、コンプライアンスチームはリスクを特定の IT 資産またはサービスに自動的にリンクできるようになり、特にテクノロジーリスクとサードパーティの依存関係のコンテキストで、より正確なリスクアセスメントを確実に行うことができます。
- アラートのノイズリダクションと自動化: ITOM AIOps を活用して、関連するアラート (インフラストラクチャ障害など) を自動的にグループ化して関連付けることで、アラートによる疲弊を軽減しました。これにより、リスクチームとコンプライアンスチームが無関係なアラートをふるいにかける手作業が削減され、優先度の高いオペレーショナルリスクに集中できるようになりました。

## 主な成果

- 統一されたリスクと IT 運用: ITOM ServiceNow IRM と統合することで、機関は運用リスクと IT リスクの両方を統一して表示できるようになりました。この統合により、運用中の IT の障害に起因するリスクの特定が容易になり、重大なアラートがエスカレートする前に迅速に対処できるようになりました。
- 自動化による効率の向上: ITOM 自動化により、新たなリスクをもたらす可能性のあるサービスの中断や IT 環境の変化を手動で追跡するなど、オペレーショナルリスクの監視に関連する手動プロセスを排除できました。
- IT 関連規制へのコンプライアンスの強化: ITOM によって提供されるリアルタイムデータにより、機関は IT リスクと監査準備に関する規制要件を満たすことができました。すべての IT 資産と構成を最新の状態に保つ ITOM 機能により、監査プロセスが迅速かつ正確になりました。
- 将来のリスク管理ニーズに対応するスケーラビリティ: ITOM のクラウドネイティブアーキテクチャはスケーラビリティと柔軟性を提供し、金融機関が成長に合わせてリスクを管理し続けることができるようにしました。また、ITOM はモバイルアクセスもサポートし、リスクチームと IT チームによるリモート監視とアラート管理を可能にしました。

## ハードウェア資産管理と持続可能な IT

持続可能な IT アプリケーションを使用すると、ハードウェア資産によって発生する排出量を効果的に管理および監視できます。さらに、資産のエネルギー消費量と、資産が寿命に達した後の適切な廃棄を追跡できます。

### ハードウェア資産管理と ESG Management を統合することの複合的なメリット 持続可能な IT

機能	ハードウェア資産管理	ESG Management	すべてのアプリケーションをまとめる
ハードウェア資産インベントリ管理	✔		✔

機能	ハードウェア資産管理	ESG Management	すべてのアプリケーションをまとめる
ハードウェア資産のエネルギー消費と排出量を推定する			
ハードウェア資産のライフサイクルトラッキング			
電子廃棄物の削減を報告する			
ポートフォリオ内の Energy Star 認定資産の割合を増やす			
データセンターのエネルギー消費、炭素排出量、再生可能エネルギーを追跡する			
ターゲットを絞った改善のために、各場所からPUE、WUE、およびCUEを監視			
関連するすべての持続可能な IT 測定基準を一目で追跡			

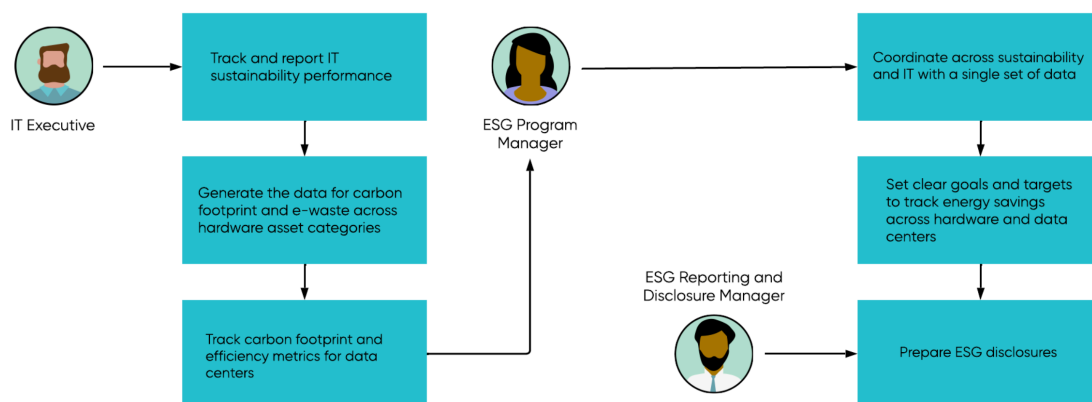
## ハードウェア資産管理と持続可能な IT

ハードウェア資産管理アプリケーションと持続可能な ITアプリケーションを一緒に使用すると、次のようなメリットがあります。

- ハードウェア資産によって発生する排出量を効果的に管理および監視できます
- 資産のエネルギー消費量と、資産が寿命に達した後の適切な廃棄を追跡するのに役立ちます。
- ダッシュボードを通じて貴重なインサイトを提供し、これらの資産を廃止するか再利用するかについて、情報に基づいた意思決定を行うことができます

この図は、二酸化炭素排出量と電子廃棄物に関するデータを収集する上での IT 担当役員と持続可能性プログラムマネージャーの共同作業を示しています。ESGプログラムマネージャーは、省エネ対策の有効性を監視し、開示を作成するための目標とターゲットを設定します。

ハードウェア資産管理および持続可能な ITワークフロー



このワークフローの場合：






1. IT 担当役員は、資産担当役員ワークスペースにログインして、IT の持続可能性パフォーマンスを追跡および報告します。
2. 次に、ITエグゼクティブは、さまざまなハードウェア資産カテゴリで発生した二酸化炭素排出量と電子廃棄物を取得し、データセンターの二酸化炭素排出量と効率の指標を追跡します。
3. ESG プログラムマネージャーは、単一の共有データセットを使用して持続可能性と IT を調整します。
4. ESG プログラムマネージャーは、省エネ対策の有効性を監視するための目標とターゲットを設定し、ESG 報告および開示マネージャーが開示を準備するのを支援します。
5. ESG レポートおよび開示マネージャーは、ESG 開示を準備します。

## ハードウェア資産管理と ESG Management を統合するための要件

1. 持続可能な IT (sn\_esg\_sustain) プラグインをインストールしてアクティブ化します。
2. ハードウェア資産管理 (sn\_hamp) プラグインをインストールしてアクティブ化します。

持続可能な IT を使用して IT 資産からの排出量データを追跡し始める

持続可能な ITを開始するには、次のタスクを完了します。

1. Activate the Sustainable IT plugin 。
2. 持続可能な IT メトリクスの定義をフィルターしてアクティブ化します 。
3. Create new entities for data centers 。
4. Manually set up entities for Sustainable IT data centers 。
5. Configure Sustainable IT 。

## オンボーディングプロセス中にサプライヤーを評価することで リスクを最小限に抑える

Risk Assessments Integration for サプライヤーライフサイクルオペレーション を使用すると、新しいサプライヤーのオンボーディング時に潜在的なサプライヤーリスクを特定して評価できます。

サプライヤーライフサイクルオペレーションを統合することの複合的なメリット  
サードパーティリスク管理

機能	サプライヤーライフサイクルオペレーション	サードパーティリスク管理	すべてのアプリケーションをまとめる
サプライヤーオンボーディング			
情報およびデータ管理			
ケースと異議申し立ての管理			
リスクオンボーディング			

機能	サプライヤーライフサイクルオペレーション	サードパーティリスク管理	すべてのアプリケーションをまとめる
サードパーティリスクデューデリジェンス、外部および内部リスクアセスメント			
リスクインテリジェンス			
リスクのスコアリングと監視			
リスク担当役員ダッシュボード			

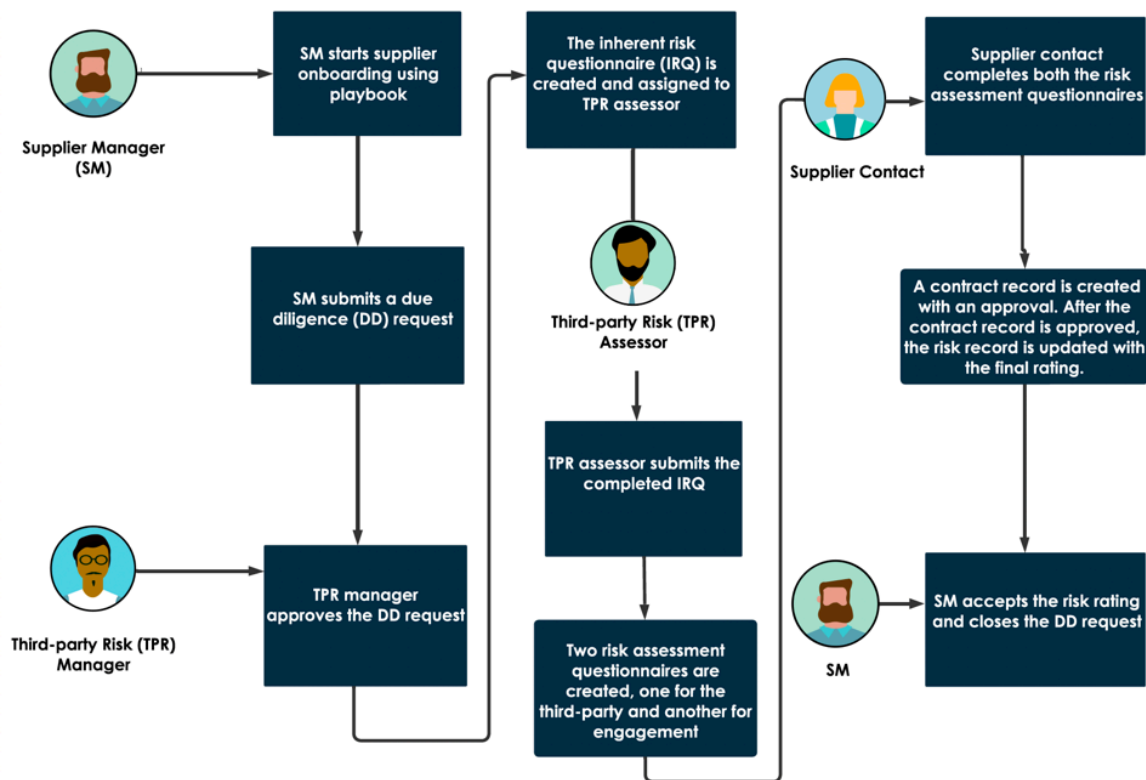
### のリスクアセスメント統合のワークフロー サプライヤーライフサイクルオペレーション

サプライヤーライフサイクルオペレーション と サードパーティリスク管理 を併用すると、次のメリットが得られます。

- サプライヤーオンボーディング時のサプライヤーリスクの評価
- リスクスコアを分析してサプライヤーをオンボーディングするかどうかを決定します

次の図は、サプライヤーマネージャーとサードパーティリスク (TPR) 査定人がアプリケーションを組み合わせて使用してサプライヤーリスクを評価する方法のワークフロー例を示しています。

サプライヤーライフサイクルオペレーションおよびサードパーティリスク管理ワークフロー



このワークフローの場合：

1. サプライヤーマネージャーは、サプライヤーオンボーディング要求を受信します。
2. サプライヤーマネージャーは、サプライヤーをオンボーディングするための簡素化されたガイド付きプロセスを提供するオンボーディングプレイブックを使用します。詳細については、「[Use the supplier onboarding playbook to onboard suppliers](#)」を参照してください。
3. サプライヤーマネージャーがデューデリジェンス要求を送信します。  
  
デューデリジェンスの実行は、サプライヤーをオンボーディングする際の重要な側面です。サプライヤーリスクアセスメントは、サードパーティリスク (TPR) 査定人によって行われます。詳細については、「[サプライヤーライフサイクルオペレーションのリスクアセスメント統合の開始](#)」を参照してください。
4. TPR マネージャーがデューデリジェンス要求を承認します。
5. 固有リスクアンケートが作成され、TPR 査定人にアサインされます。
6. TPR 査定人は、完成した IRQ を提出します。
7. 2 つのリスクアセスメントアンケートが作成され、サプライヤー連絡先にアサインされます。
8. サプライヤー連絡先は Supplier Collaboration Portal にログインし、リスクアセスメントアンケートに回答します。
9. 承認を含む契約レコードが作成されます。契約レコードが承認されると、リスクレコードが最終評価で更新されます。
10. サプライヤーマネージャーはリスク評価を受け入れ、デューデリジェンス要求をクローズします。

## サプライヤーライフサイクルオペレーションとサードパーティリスク管理を統合するための要件

1. ServiceNow Store から サプライヤーライフサイクルオペレーション (com.snc.sn\_supplier\_mgmt) アプリケーションをインストールします。詳細については、「[Install Supplier Case Management](#)」を参照してください。
2. サプライヤーライフサイクルオペレーションのリスクアセスメント統合 (com.snc.sn\_supplier\_tprm) プラグインをインストールしてアクティブ化します。
3. ServiceNow Store から サードパーティリスク管理 (com.sn\_vdr\_risk\_asmt) アプリケーションをインストールします。詳細については、「[Configuring Third-party Risk Management](#)」を参照してください。
4. GRC: サードパーティのデューデリジェンス要求 (com.sn\_tprm\_onboarding) プラグインをインストールしてアクティブ化します。

### **i** 注:

この Better Together ソリューションを利用するには、サードパーティリスク管理 (以前の Vendor Risk Management) のライセンスが必要です。

## のリスクアセスメント統合を開始する サプライヤーライフサイクルオペレーション

サプライヤーライフサイクルオペレーション のリスクアセスメント統合を開始するには、次のタスクを完了します。

1. サプライヤーを作成します。詳細については、「[Create a supplier from the Source-to-Pay Workspace](#)」を参照してください。
2. プレイブックを使用して新しいサプライヤーをオンボーディングします。詳細については、「[Use the supplier onboarding playbook to onboard suppliers](#)」を参照してください。
3. プレイブックはデューデリジェンス要求を作成します。このアクティビティのフィールドの詳細については、「[Request due diligence for a third-party engagement](#)」を参照してください。
4. サプライーマネージャーは、TPR マネージャーにアサインされるデューデリジェンス要求を入力して送信します。

### **i** 注:

デューデリジェンス要求ごとに、プリフィックス **DDR** で始まる一意の ID 番号がシステムによって自動的に割り当てられます。

5. デューデリジェンス要求が TPR マネージャーによって承認されると、固有のリスクに関するアンケート (IRQ) が TPR 査定人 (内部ステークホルダー) に送信されます。
6. TPR 査定人が記入済みの IRQ を送信すると、デューデリジェンスプロセスが開始されます。
7. デューデリジェンスプロセスでは 2 つのリスクアセスメントが作成され、それぞれにサードパーティ用とエンゲージメント用の外部デューデリジェンスアンケートが含まれます。
8. サプライヤー連絡先が Supplier Collaboration Portal から外部アンケートを完了して送信すると、TPR マネージャーはアンケートを確認し、デューデリジェンス要求を承認します。詳細については、「[Complete a risk assessment from the Supplier Collaboration Portal](#)」を参照してください。
9. 承認を含む契約レコードが作成されます。契約レコードが承認されると、リスクレコードが最終評価で更新されます。
10. サプライーマネージャーがリスク評価を受け入れると、デューデリジェンス要求が正常に処理および承認されたことを通知するメールが要求者に送信されます。

11. サプライヤーマネージャーがデューデリジェンス要求 (ケース) をクローズします。
12. サプライヤーマネージャーは、リスクアセスメント結果データを他のデータと組み合わせて使用し、オンボーディングプロセスを続行するかキャンセルするかを決定できます。

[store-future: BEGIN review]

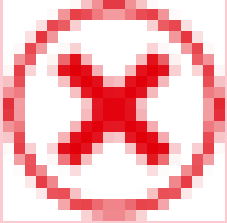

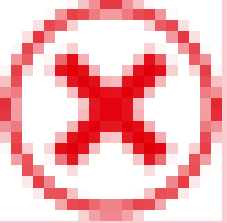
## 技術リスク、技術的負債、およびアプリケーションコストの削減

アプリケーションポートフォリオを分析し、リフレッシュサイクルを管理し、エンタープライズアーキテクチャワークスペース、IT Asset Management、および Information Technology Operations Management

エンタープライズアーキテクチャワークスペースを**IT Asset Management**と統合することの複合的なメリット**IT Operations Management (ITOM)**

機能	EA ワークスペース	ITAM	ITOM	すべてのアプリケーションをまとめる
構成アイテム (CI) の検出			 ソフトウェアとハードウェアのインベントリを検出	ITOM ディスカバリーは、ビジネスアプリケーションやアプリケーションサービスなどのハードウェアとソフトウェアの構成アイテムを識別して CMDB に追加します。  ディスカバリーは、ソフトウェアとハードウェアの最新のインベントリを提供します。APM を使用すると、アプリケーションインベントリを完全に可視化できます。
サービスマッピング			 インフラストラクチャをビジネス機能にマッピングします。	サービスマッピングは、アプリケーションインスタンスと検出されたインフラストラクチャの関係を提供します。サービスマッピングは、アプリケーションをサポートする検出された CI (本番、開発環境、およびテス

自動翻訳

機能	EA ワークスペース	ITAM	ITOM	すべてのアプリケーションをまとめる
				ト環境用のアプリケーションインスタンスまたはアプリケーションサービス) にビジネスサービスコンテキストの依存関係を作成します。
標準化されたソフトウェアおよびハードウェア製品モデルのライフサイクルコンテンツ				<p>ソフトウェア資産管理 (SAM) は、アプリケーションサービスをサポートするソフトウェアモデルの正規化されたインベントリを作成します。APM のテクノロジーポートフォリオ管理 (TPM) では、SAM ソフトウェアインベントリを使用してベンダーのライフサイクルを管理します。</p> <p>APM の一環として、Technology Portfolio Management 機能は、SAM/HAM のソフトウェアとハードウェアのライフサイクルデータを利用して、サポートされていないソフトウェアやハードウェアに依存していることによって技術的なリスクにさらされているビジネスアプリケーションをプロアクティブに特定します。</p>

- APM はこの機能を活用して、ビジネスアプリケーションに関連するリスク (可用性の損失など) を可視化し、適用されるコントロールを追跡して、アプリケーションが規制に準拠しているかどうかをテストします。- 継続的なコンプライアンス監視により、これらのアプリケーションが正しいコントロールに対して証明されていることを確認します。そのため、ビジネスアプリケーションの運用し

ジリエンスを確保できます。 - 攻撃の頻度と重大度のレベルが増し続けると、組織は大量のセキュリティアラートに圧倒され、脅威の迅速な優先順位付けと解決が困難になる可能性があります。

## エンタープライズアーキテクチャワークスペースのワークフロー

エンタープライズアーキテクチャワークスペースとIT Asset ManagementとIT Operations Management (ITOM)を併用すると、次のメリットが得られます。

- エンタープライズアーキテクトが、基盤となるテクノロジーのバージョンとライフサイクルの追跡を自動化し、期限切れまたは提供終了のテクノロジーが原因でリスクにさらされているビジネスアプリケーションを特定できるようにします。
- アプリケーションインベントリの可視化が向上します。冗長なアプリケーションや古いアプリケーションを見つけ出し、それに応じて迅速な決定を下します。
- 実行可能なワークフローを推進して、使用されなくなったライセンスへの過剰な支出を防止します。

## エンタープライズアーキテクチャワークスペース、IT Asset Management、およびIT Operations Management (ITOM)

- エンタープライズアーキテクチャワークスペース (sn\_apm\_ws) アプリケーションをインストールします。
- テクノロジーポートフォリオ管理 (sn\_apm\_tpm) アプリケーションをインストールします。
- ソフトウェア資産管理プロ (com.sn\_samp\_master) アプリケーションをインストールします。
- ハードウェア資産管理 (com.sn\_hamp) アプリケーションをインストールします。

## 企業のテクノロジーリスクの評価の概要

テクノロジーリスクの評価を開始するには、次の手順に従います。

1. ビジネスアプリケーションのテクノロジーを戦略的ビジネスイニシアチブに合わせます。スケジュール済みジョブを実行して、テクノロジーポートフォリオのテクノロジーライフサイクルデータをフェッチできます。「[Run a scheduled job to generate TPM lifecycle data - Legacy](#)」を参照してください。
2. EA ワークスペースの [インサイト] セクションの [テクノロジーポートフォリオ] タブで、ビジネスアプリケーション、アプリケーションサービス、サーバー、ソフトウェア製品、およびハードウェアモデルのテクノロジーライフサイクルリスクを表示します。これらのテクノロジーライフサイクルリスクをフィルタリングして、関心のあるアプリケーションのみを表示できます。「[Viewing insights of your portfolio](#)」を参照してください。
3. TPM 検出テクノロジー実行ログ [sn\_apm\_tpm\_discovered\_technology\_run\_log] テーブルを調べて、テクノロジーポートフォリオ管理 (TPM) 分析の進捗状況を追跡します。分析が実行されるたびに、このテーブルにエントリが追加されます。実行ログを表示するには、EA ワークスペースでポートフォリオ リストビュー (EA ワークスペース>ポートフォリオ>テクノロジーポートフォリオ管理>ログ) に移動します。「[Exploring Portfolio list view](#)」を参照してください。
4. ビジネスアプリケーションを合理化して、複数のスコアに基づいてビジネスアプリケーションを分析し、ビジネスアプリケーションのデマンドを作成し、ビジネスアプリケーションの予定されている廃棄を設定し、ライフサイクルの詳細を既存のビジネスアプリケーションに追加します。「[Rationalization of business applications](#)」を参照してください。

[End]