



Yokohama é Melhor Juntos

Última atualização: 17/12/2025

Tradução automática

A tradução automática pode proporcionar uma ideia básica do conteúdo em um idioma que você entende. Ela é totalmente automatizada e não envolve intervenção humana. A qualidade e a precisão da tradução automática podem variar significativamente de um texto para outro e entre diferentes pares de idiomas. A ServiceNow não garante a precisão e não se responsabiliza por possíveis erros. Alguns conteúdos (como imagens, vídeos, arquivos etc.) podem não ser traduzidos devido a limitações técnicas do sistema.

Alguns exemplos e gráficos aqui representados são fornecidos somente para fins de ilustração. Nenhuma associação ou conexão real com produtos ou serviços ServiceNow é intencional ou deve ser inferida.

ServiceNow, o logotipo ServiceNow, Now e outras marcas ServiceNow são marcas comerciais e/ou marcas registradas da ServiceNow, Inc. nos Estados Unidos e/ou em outros países. Outros nomes de empresas e de produtos podem ser marcas comerciais das respectivas empresas às quais estão associados.

Leia os Termos de Uso do Site do ServiceNow em www.servicenow.com/terms-of-use.html

Tradução automática

Sede da empresa
2225 Lawson Lane
Santa Clara, CA 95054
Estados Unidos
(408) 501-8550

Índice

Soluções.....	4
Melhore a visibilidade da exposição a riscos organizacionais com a avaliação avançada de riscos do projeto.....	4
Como automatizar e otimizar seus serviços e operações usando o Espaço de operações de serviços.....	7
Estudo de caso: aprimoramento de risco, conformidade e Gestão de auditorias com ITOM.....	12
Rastreie o desempenho de seus ativos de TI usando Gestão de ativos de hardware e TI sustentável.....	13
Minimize o risco avaliando os fornecedores durante o processo de integração.....	16
Reduza o risco de tecnologia, a dívida técnica e os custos de aplicação.....	21
[store-future: BEGIN review]	
[End]	

Tradução automática

Soluções

Com as Soluções, aprimore a funcionalidade das aplicações ServiceNow usando-as em combinação entre si.


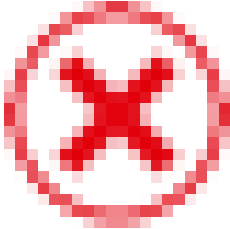

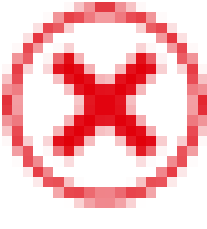
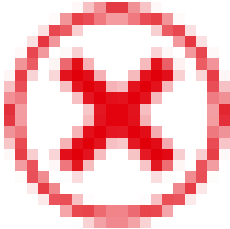




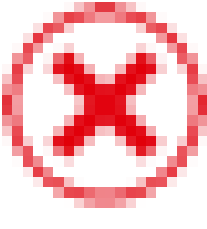
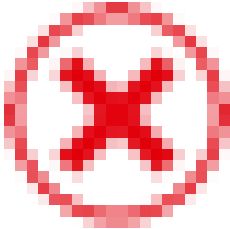

Soluções disponíveis

Saiba mais sobre os benefícios de cada solução e como implementá-las e usá-las.

Melhore a visibilidade da exposição a riscos organizacionais com a avaliação avançada de riscos do projeto

Com a avaliação de risco avançada para seus projetos, você pode identificar facilmente se algum projeto representa possíveis riscos organizacionais e decidir rapidamente sobre as ações de mitigação. Combine a gestão de riscos do projeto com a gestão de riscos empresariais e obtenha melhor visibilidade sobre a exposição geral ao risco da sua organização.

Benefícios combinados da integração de Project Portfolio Management com Risco avançado

Funcionalidade	Project Portfolio Management	Risco avançado	Ambas as aplicações juntas
Avaliação de risco do projeto			
Elevação para risco empresarial			
Avaliação de riscos inerentes e residuais			
Registros integrados de projeto e risco empresarial			

Tradução automática

Funcionalidade	Project Portfolio Management	Risco avançado	Ambas as aplicações juntas
Mapas térmicos de risco			
Painel de visão geral de risco do projeto empresarial			

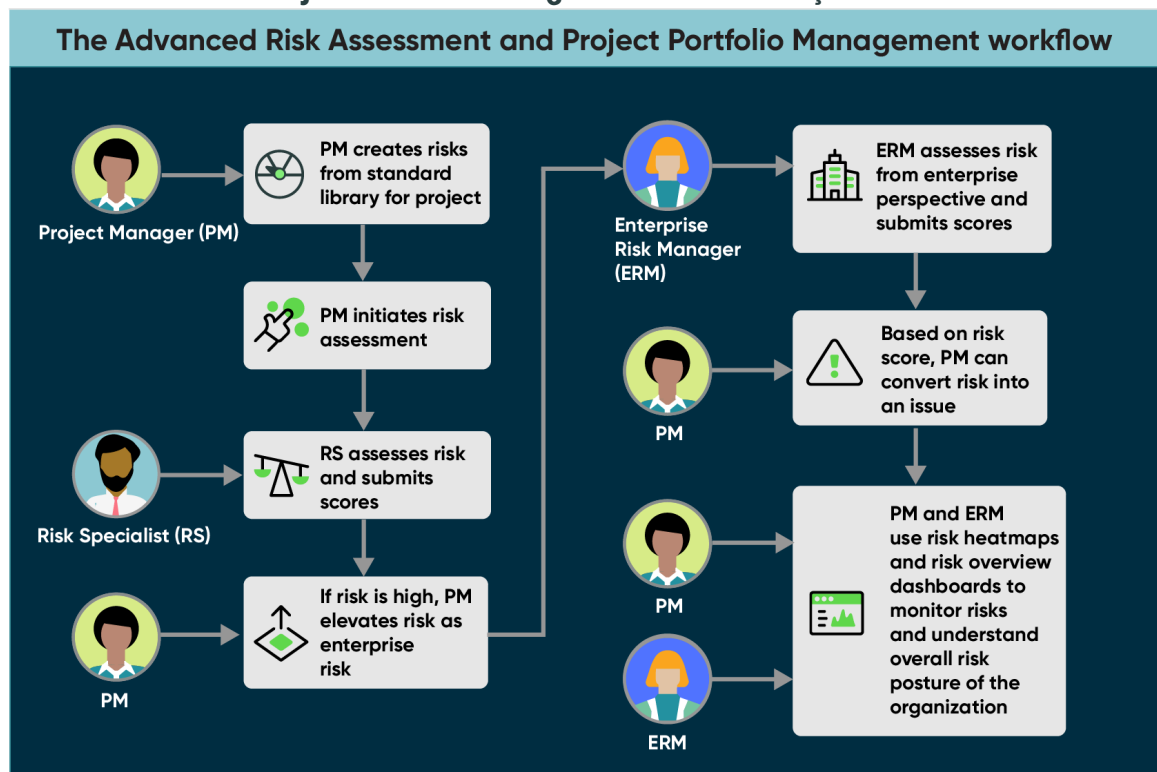
Fluxo de trabalho de avaliação de risco avançada do projeto

Use Project Portfolio Management (PPM) e Risco avançado Avaliação (ARA) juntos para obter estes benefícios:

- Monitore sua exposição a riscos no nível da organização
- Integre seu sistema de gestão de riscos para as equipes de risco do projeto e da empresa.

A figura a seguir mostra um exemplo de fluxo de trabalho de como um gerente de projeto, um especialista em risco e um gerente de riscos empresariais usam as aplicações juntos para avaliar e mitigar riscos no nível do projeto e da empresa.

O fluxo de trabalho Project Portfolio Management e Risco avançado



Tradução automática

Neste fluxo de trabalho:

1. O gerente de projeto cria riscos da biblioteca padrão para o projeto e inicia a avaliação de risco.
2. O especialista em risco avalia o risco e atribui a ele uma pontuação de avaliação.
3. Se a pontuação de risco for alta, o gerente de projeto elevará o risco como um risco corporativo.
4. O gerenciador de riscos empresariais avalia o risco da perspectiva da empresa e atribui a ele uma pontuação de avaliação.
5. Com base na pontuação de risco, o gerente de projeto pode converter o risco em um problema.
6. O gerente de projeto e o gerente de riscos empresariais usam mapas térmicos de risco e painéis de visão geral de risco para monitorar os riscos e entender a postura geral de risco da organização.

Requisitos para integração Project Portfolio Management e Risco avançado

1. Ative o plug-in Project Portfolio Management [com.snc.financial_planning_pmo].
2. Instale a aplicação GRC: Advanced Risk a partir do ServiceNow® Store.

Introdução à avaliação de risco de projeto avançada

Para começar a avaliar os riscos do projeto, siga estas etapas:

1. Instale e configure a metodologia de avaliação de risco. Consulte [Configuração da integração Project Portfolio Management e Advanced Risk](#) .

Função: sn_risk.admin.

2. Defina o escopo e inicie a avaliação de risco. Consulte [Como adicionar riscos a um projeto](#) .

Função: it_project_manager.

3. Executar avaliação de risco. Consulte [Realizar avaliação de risco](#) .

Função: sn_grc.business_user.

4. Avalie e eleve para o risco do projeto. Consulte [Elevação de um risco de projeto para risco corporativo](#) .

Função: it_project_manager.

5. Converta o risco em problema e monitore a postura de segurança. Consulte [Monitorar postura de risco](#) .






Função: sn_risk.admin, it_project_manager.

Como automatizar e otimizar seus serviços e operações usando o Espaço de operações de serviços

Você pode expandir os serviços enquanto reduz custos, proporcionando experiências de alta qualidade para clientes e funcionários e impulsionando a resiliência operacional. Use uma única plataforma de nuvem que integra processos de TI, como incidente, problema e mudança, com operações de TI, como descoberta, definições de serviço de negócios, mapeamento de serviços e gestão de eventos.

Benefícios combinados da integração de Espaço de operações de serviços para Gestão de serviços de TI (ITSM) e IT Operations Management (ITOM)

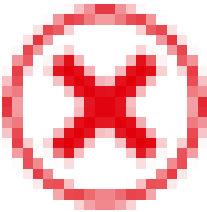

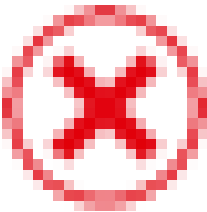


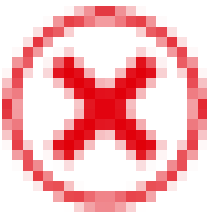


Benefits with Service Operations Workspace for ITSM and ITOM

-  Provides a unified experience for services and operations
-  Eliminates silos by connecting services and operations teams
-  Creates and extends processes using low-code configuration
-  Increases productivity and keeps employees engaged
-  Optimizes processes for faster resolution of outages and incidents

Funcionalidade	Espaço de operações de serviços para ITSM	Espaço de operações de serviços para ITOM	Todas as aplicações juntas
IU (User Interface, interface do usuário) simples, intuitiva e clara	✓	✓	✓

Funcionalidade	Espaço de operações de serviços para ITSM	Espaço de operações de serviços para ITOM	Todas as aplicações juntas
Recomendações automatizadas com base nas ações do usuário	✓	✓	✓
Página principal personalizada que fornece uma visão geral das tarefas	✓	✓	✓
Gestão de incidentes eficaz para agentes da central de serviços	✓	✗	✓
Especialistas de plantão para tarefas de alta prioridade	✓	✗	✓
Experiência de integração para usuários conectados	✓	✓	✓
Walk-Up Experience	✓	✗	✓
Gestão de solicitações a partir de incidentes e interações	✓	✗	✓
Experiência guiada para configuração inicial do Espaço de operações de serviços	✓	✗	✓

Tradução automática

Funcionalidade	Espaço de operações de serviços para ITSM	Espaço de operações de serviços para ITOM	Todas as aplicações juntas
Apresentação do contexto completo de um serviço com métricas relacionadas, logs e informações adicionais			
Correção rápida de alertas de um serviço			
Automação rápida para operadores ao usar uma experiência de playbook integrada nos formulários de alerta			

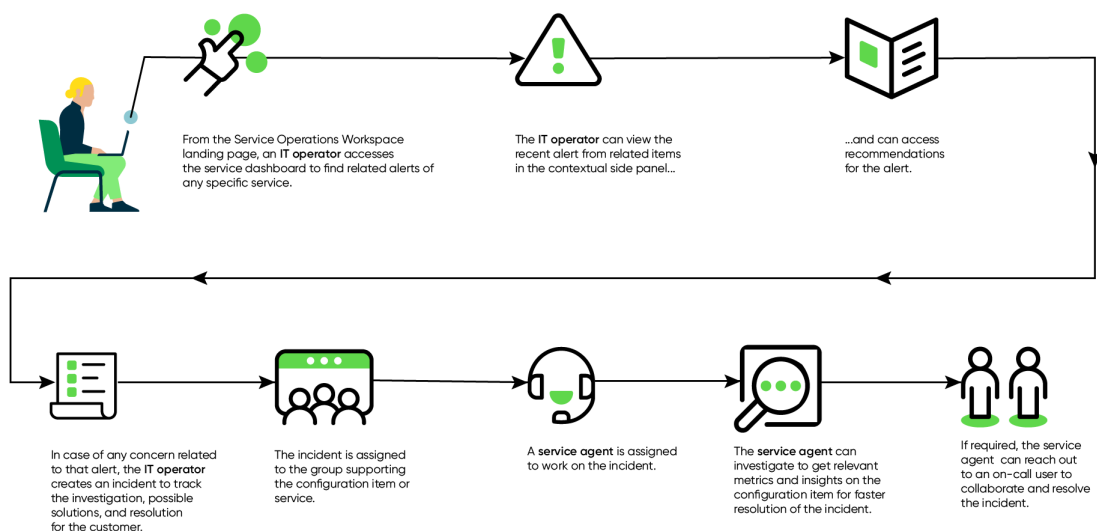
Fluxo de trabalho para Espaço de operações de serviços

Use Espaço de operações de serviços para Gestão de serviços de TI (ITSM) e IT Operations Management (ITOM) juntos para estes benefícios:

- Forneça uma experiência unificada para serviços e operações em uma única plataforma.
- Elimine silos conectando serviços e equipes de operações.
- Aumente a produtividade e mantenha os funcionários engajados.
- Crie e estenda processos ITSM e ITOM com configuração low-code.
- Otimize os processos ITSM e ITOM para uma resolução mais rápida de incidentes e indisponibilidades.

A figura a seguir mostra um exemplo de fluxo de trabalho de como um operador de TI e um agente de serviço (agente da central de serviços ou especialista L2/L3) podem usar essas aplicações para resolver um problema do cliente.

Espaço de operações de serviços para fluxos de trabalho ITSM e ITOM



Neste fluxo de trabalho:

1. Na página principal Espaço de operações de serviços, um operador de TI acessa o painel de serviço para encontrar alertas relacionados a qualquer serviço específico.
2. O operador de TI pode exibir o alerta recente de itens relacionados no painel lateral contextual.
3. O operador de TI pode acessar recomendações para o alerta.
4. Se houver algum problema do cliente relacionado a esse alerta, o operador de TI criará um incidente para rastrear a investigação, as possíveis soluções e a resolução para o cliente.
5. O incidente é atribuído ao grupo que oferece suporte ao item de configuração ou serviço.
6. Um agente de serviço, como um agente de central de serviços ou especialista L2/L3, é atribuído para trabalhar no incidente.
7. O agente de serviço pode investigar para obter métricas e informações relevantes sobre o item de configuração para uma resolução mais rápida do incidente.
8. Se necessário, o agente de serviço pode entrar em contato com um usuário de plantão para colaborar e resolver o incidente.

Requisitos para integração Espaço de operações de serviços de para ITSM e ITOM

1. Certifique-se de que as seguintes condições sejam atendidas para Espaço de operações de serviços para ITSM.
 - a. Adquira a ITSM licença padrão ou posterior para ServiceNow® Gestão de serviços de TI aplicações. Entre em contato com seu ServiceNow gerente de contas ou representante de vendas.
 - b. Se você quiser usar o Framework de investigação em Espaço de operações de serviços para ITSM, adquira a licença ITSM Professional ou posterior para aplicações ServiceNow® Gestão de serviços de TI.
 - c. Instale Espaço de operações de serviços ITSM aplicações do ServiceNow® Store. Para obter informações sobre como instalar esta aplicação, consulte [Instalar aplicações do Espaço de operações de serviços ITSM](#).
2. Certifique-se de que as seguintes condições sejam atendidas para Espaço de operações de serviços para ITOM.
 - a. Adquira a licença ITOM Professional ou posterior para aplicações ServiceNow® IT Operations Management. Entre em contato com seu ServiceNow gerente de contas ou representante de vendas.
 - b. Instale Espaço de operações de serviços ITOM aplicações do ServiceNow® Store. Para obter informações sobre como instalar esta aplicação, consulte [Instalação do Espaço de operações de serviços para aplicações ITOM](#) .

Comece com Espaço de operações de serviços para ITSM e ITOM

Para começar com Espaço de operações de serviços para ITSM e ITOM, siga estas etapas:

1. Configure Espaço de operações de serviços para ITSM.
 - a. Configure Espaço de operações de serviços para ITSM. Consulte [Como configurar o Espaço de operações de serviços para ITSM](#).
Função: administrador.
 - b. Configure o Framework de investigação. Consulte [Como configurar o Framework de investigação no Espaço de operações de serviços](#) .
Função: administrador.
 - c. Configure a Estrutura de recomendação para um incidente. Consulte [Como configurar a Estrutura de recomendação no Espaço de operações de serviços para ITSM](#) .
Função: administrador.
2. Configure Espaço de operações de serviços para ITOM.
 - a. Configure Espaço de operações de serviços para ITOM. Consulte [Configuração do Espaço de operações de serviços para ITOM](#).
Função: evt_mgmt_operator.
 - b. Configure as métricas de alerta. Consulte [Configuração de métricas de alerta](#) .
Função: evt_mgmt_operator.

- c. Configure a Estrutura de recomendação para um alerta. Consulte [Como configurar a Estrutura de recomendação no Espaço de operações de serviços para ITOM](#).

Função: evt_mgmt_admin.

- d. Configure a caixa de entrada Espaço de operações de serviços. Consulte [Configuração da caixa de entrada no Espaço de operações de serviços para ITOM](#).

Função: evt_mgmt_admin.

- e. Personalize Espaço de operações de serviços listas. Consulte [Personalizar listas no Espaço de operações de serviços para ITOM](#) .

Função: itil.

Estudo de caso: aprimoramento de risco, conformidade e Gestão de auditorias com ITOM

O caso de uso demonstra como a integração ITOM simplificou a gestão de riscos, conformidade e auditoria para uma instituição financeira, fornecendo visibilidade operacional em tempo real, automação e avaliações de risco aprimoradas.

Declaração do problema

Uma instituição financeira líder buscou simplificar seus processos de gestão de riscos conforme aumentava, lidando com riscos operacionais, de terceiros e de tecnologia cada vez mais complexos, junto com funções de conformidade e auditoria interna. A instituição reconheceu a necessidade de uma plataforma unificada para melhorar a eficiência e reduzir o esforço manual.

Desafios

- Falta de visibilidade centralizada: a instituição financeira encontrou desafios para manter uma visão clara e em tempo real dos riscos, conformidade e processos de auditoria. Sistemas diferentes dificultaram a avaliação de riscos operacionais vinculados a serviços e infraestrutura de TI.
- Infraestrutura de TI isolada: os sistemas de TI desconectados da instituição tornavam difícil monitorar e responder a problemas operacionais que podem afetar as funções de gestão de riscos, como tempos de inatividade, erros de configuração e falhas de serviço de TI.
- Uso limitado dos dados existentes: a quantidade significativa de dados de TI disponíveis de várias fontes não foi totalmente utilizada para gestão de riscos e conformidade devido à falta de integração com os sistemas existentes.

Soluções específicas de ITOM

- Visibilidade operacional em tempo real: ITOM forneceu à instituição informações em tempo real sobre a integridade, a disponibilidade e o desempenho dos serviços de TI. Ao integrar ITOM com ServiceNow IRM, as equipes de risco e conformidade foram capazes de correlacionar riscos operacionais (por exemplo, indisponibilidades de serviço, degradação de desempenho) diretamente com esforços mais amplos de gestão de riscos.
- Automatizado Mapeamento de serviços para melhor avaliação de risco: as capacidades Mapeamento de serviços em ITOM permitiram que a instituição mapeasse automaticamente

os serviços de TI e entendesse suas dependências. Isso foi essencial para avaliar os riscos operacionais em tempo real. Por exemplo, o sistema pode detectar uma falha crítica de serviço e sinalizá-la imediatamente como um evento de alto risco no painel de conformidade, permitindo que a instituição tome medidas preventivas.

- **Monitoramento proativo e resposta de alerta:** ao aproveitar ITOM Gestão de eventos, a instituição conseguiu monitorar os principais riscos operacionais, como falhas do sistema e indisponibilidades de serviços de terceiros, e acionar alertas automatizados para as equipes relevantes de gestão de riscos e conformidade. Essa abordagem proativa minimizou o tempo entre a identificação de um risco operacional e a resposta a ele.
- **Configuration Management Database (CMDB) para Conformidade:** a integração de ITOM com CMDB assegurou que todos os ativos de TI, configurações e seus relacionamentos fossem rastreados com precisão. Isso forneceu uma única fonte de verdade para a gestão de riscos, permitindo que as equipes de conformidade vinculem automaticamente os riscos a ativos ou serviços de TI específicos, garantindo avaliações de risco mais precisas, especialmente no contexto de riscos de tecnologia e dependências de terceiros.
- **Redução e automação de ruídos de alerta:** ITOM O AIOps foi aproveitado para reduzir o esgotamento de alertas, agrupando e correlacionando automaticamente alertas relacionados (por exemplo, de falhas de infraestrutura). Isso reduz o esforço manual das equipes de risco e conformidade para filtrar alertas irrelevantes, permitindo que elas se concentrem nos riscos operacionais de maior prioridade.

Principais resultados

- **Risco unificado e operações de TI:** ao integrar ITOM com ServiceNow IRM, a instituição obteve uma visão unificada dos riscos operacionais e de TI. Essa integração facilitou a identificação de riscos decorrentes de falhas operacionais de TI, ajudando a instituição a lidar rapidamente com alertas críticos antes que eles aumentassem.
- **Maior eficiência por meio da automação:** ITOM a automação ajudou a instituição a eliminar processos manuais relacionados ao monitoramento de riscos operacionais, como o acompanhamento manual de interrupções de serviço ou mudanças no ambiente de TI que podem introduzir novos riscos.
- **Conformidade aprimorada com regulamentações relacionadas a TI:** os dados em tempo real fornecidos por ITOM garantiram que a instituição atendesse aos requisitos regulatórios em relação aos riscos de TI e à prontidão para auditoria. A capacidade de ITOM de manter todos os ativos e configurações de TI atualizados tornou os processos de auditoria mais rápidos e precisos.
- **Escalabilidade para necessidades futuras de gestão de riscos:** a arquitetura nativa da nuvem de ITOM forneceu escalabilidade e flexibilidade, garantindo que a instituição continuasse a gerenciar os riscos conforme aumentava. ITOM também oferece suporte ao acesso móvel, permitindo o monitoramento remoto e o gerenciamento de alertas pelas equipes de risco e TI.

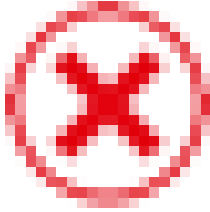
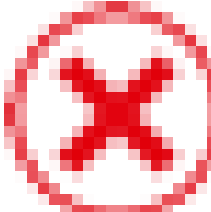

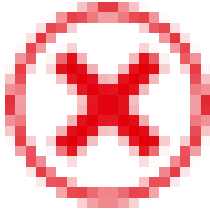
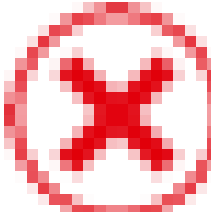

Rastreie o desempenho de seus ativos de TI usando Gestão de ativos de hardware e TI sustentável

A aplicação TI sustentável permite que você gerencie e monitore com eficácia as emissões geradas por seus ativos de hardware. Além disso, permite que você acompanhe o consumo de energia de seus ativos e o descarte adequado depois que eles atingem o fim da vida útil.

Benefícios combinados da integração Gestão de ativos de hardware de e Gestão de ESG de TI sustentável

Funcionalidade	Gestão de ativos de hardware	Gestão de ESG	Todas as aplicações juntas
Gestão de inventário de ativos de hardware			
Estime o consumo de energia e as emissões de ativos de hardware			
Acompanhamento do ciclo de vida de ativos de hardware			
Relatar redução no lixo eletrônico			
Aumentar a proporção de ativos certificados pela Energy Star no portfólio			
Rastreie o consumo de energia, carbono e energias renováveis do datacenter			

Tradução automática

Funcionalidade	Gestão de ativos de hardware	Gestão de ESG	Todas as aplicações juntas
Monitore PUE, WUE e CUE de cada local para melhoria direcionada			
Acompanhe rapidamente todas as métricas relevantes de TI sustentável			

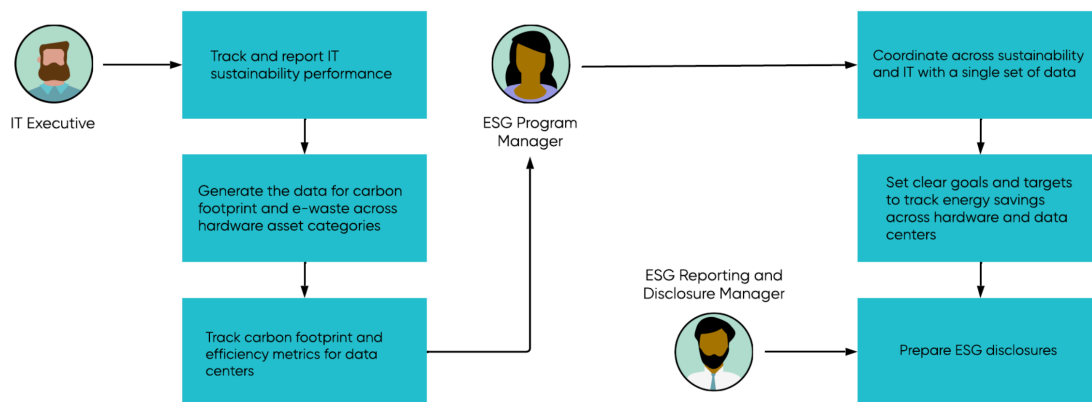
Fluxo de trabalho para usar Gestão de ativos de hardware e TI sustentável

O uso das aplicações Gestão de ativos de hardware e TI sustentável juntos oferece os seguintes benefícios:

- Permite que você gerencie e monitore com eficácia as emissões geradas por seus ativos de hardware
- Ajuda a acompanhar o consumo de energia de seus ativos e o descarte adequado depois que eles atingem o fim da vida útil.
- Fornece informações valiosas por meio de um painel, permitindo que você tome decisões informadas sobre descontinuar ou redirecionar esses ativos

A figura ilustra os esforços de colaboração entre um executivo de TI e o gerente do programa de sustentabilidade na coleta de dados sobre pegada de carbono e lixo eletrônico. Os gerentes do programa ESG estabelecem objetivos e metas para monitorar a eficácia das medidas de economia de energia e preparar divulgações.

O fluxo de trabalho Gestão de ativos de hardware e TI sustentável



Neste fluxo de trabalho:

1. O executivo de TI faz login no Espaço executivo de ativos para rastrear e relatar o desempenho de sustentabilidade de TI.
2. O executivo de TI obtém a pegada de carbono e o lixo eletrônico gerados em diferentes categorias de ativos de hardware e rastreia a pegada de carbono e as métricas de eficiência dos datacenters.
3. O gerente do programa ESG coordena entre Sustentabilidade e TI com um único conjunto compartilhado de dados.
4. Os gerentes de programa de ESG estabelecem objetivos e metas para monitorar a eficácia das medidas de economia de energia e, assim, ajudar o gerente de relatórios e divulgação de ESG a preparar divulgações.
5. O gerente de relatórios e divulgação de ESG prepara as divulgações de ESG.

Requisitos para integração de Gestão de ativos de hardware e Gestão de ESG

1. Instale e ative o plug-in TI sustentável (sn_esg_sustain).
2. Instale e ative o plug-in Gestão de ativos de hardware (sn_hamp).

Comece com usando TI sustentável para rastrear seus dados de emissões de seus ativos de TI

Comece com TI sustentável concluindo estas tarefas:

1. [Activate the Sustainable IT plugin](#) .
2. [Filtrar e ativar as definições de métrica de TI sustentável](#) .
3. [Create new entities for data centers](#) .
4. [Manually set up entities for Sustainable IT data centers](#) .
5. [Configure Sustainable IT](#) .

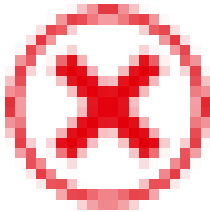


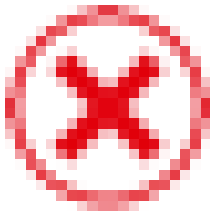


Minimize o risco avaliando os fornecedores durante o processo de integração

Com a Integração de avaliações de risco para Operações do ciclo de vida do fornecedor, você pode identificar e avaliar possíveis riscos do fornecedor ao integrar novos fornecedores.

Benefícios combinados da integração de Operações do ciclo de vida do fornecedor com Gestão de risco de terceiros

Funcionalidade	Operações do ciclo de vida do fornecedor	Gestão de risco de terceiros	Todas as aplicações juntas
Integração do fornecedor	✓	✗	✓
Gestão de informações e dados	✓	✗	✓
Gestão de casos e contestações	✓	✗	✓
Integração de risco	✗	✓	✓
Diligência prévia de risco de terceiros, avaliação de risco externo e interno	✗	✓	✓
Inteligência de risco	✗	✓	✓

Tradução automática

Funcionalidade	Operações do ciclo de vida do fornecedor	Gestão de risco de terceiros	Todas as aplicações juntas
Pontuação e monitoramento de risco			
Painel executivo de risco			

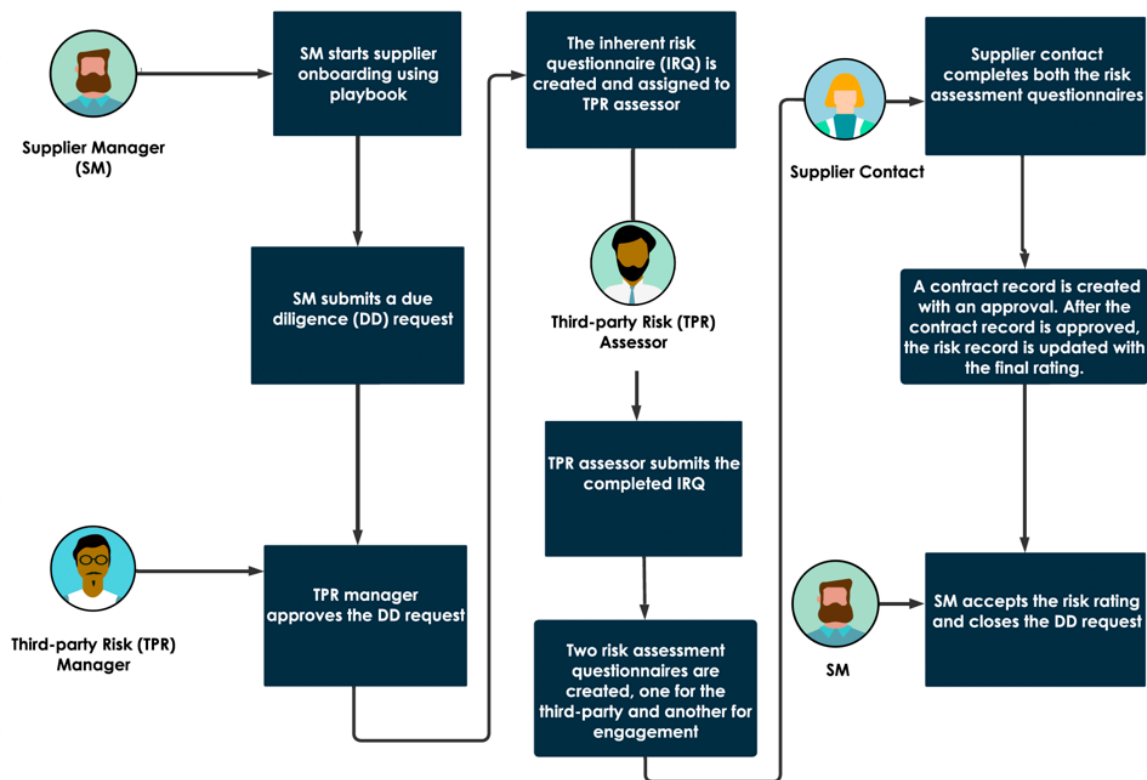
Fluxo de trabalho de integração de avaliações de risco para Operações do ciclo de vida do fornecedor

Use Operações do ciclo de vida do fornecedor e Gestão de risco de terceiros juntos para obter estes benefícios:

- Avaliar o risco do fornecedor ao integrar fornecedores
- Analisar a pontuação de risco para determinar se um fornecedor deve ser integrado

A figura a seguir mostra um exemplo de fluxo de trabalho de como um gerente de fornecedores e um avaliador de risco de terceiros (TPR) podem usar as aplicações juntas para avaliar o risco do fornecedor.

O fluxo de trabalho Operações do ciclo de vida do fornecedor e Gestão de risco de terceiros



Neste fluxo de trabalho:

1. O gerente de fornecedores recebe uma solicitação de integração do fornecedor.
2. O gerente de fornecedores usa o playbook de integração, que fornece um processo simplificado e orientado para fornecedores de integração. Para obter mais informações, consulte [Using the supplier onboarding playbook to onboard suppliers](#) .
3. O gerente do fornecedor envia uma solicitação de diligência prévia.

Realizar a diligência prévia é um aspecto fundamental da integração de um fornecedor. A avaliação de risco do fornecedor é feita pelo avaliador de risco de terceiros (TPR). Para obter mais informações, consulte [Introdução à integração de avaliações de risco para Operações de ciclo de vida do fornecedor](#).

4. O gerente de TPR aprova a solicitação de diligência prévia.
5. O questionário de risco inerente é criado e atribuído ao avaliador de TPR.
6. O avaliador de TPR envia o IRQ concluído.
7. Dois questionários de avaliação de risco são criados e atribuídos ao contato do fornecedor.
8. O contato do fornecedor faz login no Portal de colaboração com fornecedores e conclui os questionários de avaliação de risco.
9. Um registro de contrato é criado com uma aprovação. Depois que o registro do contrato é aprovado, o registro de risco é atualizado com a classificação final.
10. O gerente do fornecedor aceita a classificação de risco e encerra a solicitação de diligência prévia.

Requisitos para integração de Operações do ciclo de vida do fornecedor e Gestão de risco de terceiros

1. Instale a aplicação Operações do ciclo de vida do fornecedor (com.snc.sn_supplier_mgmt) a partir do ServiceNow® Store. Para obter mais informações, consulte [Install Supplier Lifecycle Operations](#).
2. Instale e ative o plug-in Integração de avaliações de risco para Operações de ciclo de vida do fornecedor (com.snc.sn_supplier_tprm).
3. Instale a aplicação Gestão de risco de terceiros (com.sn_vdr_risk_asmt) a partir do ServiceNow® Store. Para obter mais informações, consulte [Configuring Third-party Risk Management](#).
4. Instale e ative o plug-in GRC: solicitação de diligência prévia de terceiros (com.sn_tprm_onboarding).

i Nota:

Você deve ter uma licença para Gestão de risco de terceiros (anteriormente Vendor Risk Management) para aproveitar as vantagens desta solução da Now Now.

Introdução à integração de avaliações de risco para Operações do ciclo de vida do fornecedor

Comece com a integração de avaliações de risco para Operações do ciclo de vida do fornecedor concluindo estas tarefas:

1. Crie um fornecedor. Para obter mais informações, consulte [Create a supplier from the Source-to-Pay Workspace](#).
2. Integre um novo fornecedor usando playbooks. Para obter mais informações, consulte [Using the supplier onboarding playbook to onboard suppliers](#).
3. O playbook cria uma solicitação de diligência prévia. Para obter mais informações sobre os campos nesta atividade, consulte [Request due diligence for a third-party engagement](#).
4. O gerente do fornecedor preenche e envia uma solicitação de diligência prévia, que é atribuída ao gerente do TPR.

i Nota:

Para cada solicitação de diligência prévia, o sistema atribui automaticamente um número de ID exclusivo que começa com o prefixo **DDR**.

5. Se a solicitação de diligência prévia for aprovada pelo gerente de TPR, o questionário de risco inerente (IRQ) será enviado ao avaliador de TPR (parte interessada interna).
6. Depois que o avaliador de TPR envia o IRQ concluído, o processo de diligência prévia começa.
7. O processo de diligência prévia cria duas avaliações de risco, cada uma contendo um questionário externo de diligência prévia, um para o terceiro e outro para o compromisso.
8. Depois que os contatos do fornecedor concluem e enviam os questionários externos do Portal de colaboração com fornecedores, o gerente de TPR passa pelos questionários e aprova a solicitação de diligência prévia. Para obter mais informações, consulte [Complete a risk assessment from the Supplier Collaboration Portal](#).
9. Um registro de contrato é criado com uma aprovação. Depois que o registro do contrato é aprovado, o registro de risco é atualizado com a classificação final.

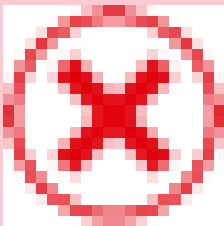
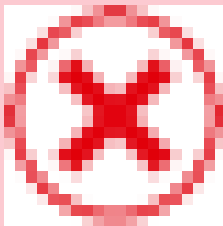

- 10. Depois que o gerente do fornecedor aceita a classificação de risco, um e-mail é enviado ao solicitante informando que a solicitação de diligência prévia foi processada e aprovada com sucesso.
- 11. O gerente do fornecedor encerra a solicitação de diligência prévia (caso).
- 12. Como gerente de fornecedores, você pode usar os dados do resultado da avaliação de risco em combinação com outros dados para determinar se deve continuar ou cancelar o processo de integração.

[store-future: BEGIN review]

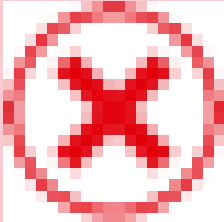
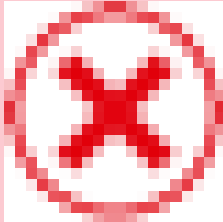

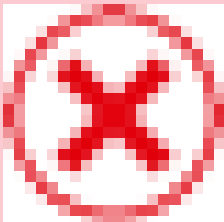

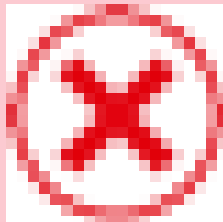
Reduza o risco de tecnologia, a dívida técnica e os custos de aplicação

Analise o portfólio de aplicações, gerencie ciclos de atualização e racionalize aplicações legadas usando Espaço de arquitetura empresarial, Gestão de ativos de TIE Information Technology Operations Management

Benefícios combinados da integração de Espaço de arquitetura empresarial com Gestão de ativos de TI e IT Operations Management

Funcionalidade	Espaço do AE	ITAM	ITOM	Todas as aplicações juntas
Descobrir itens de configuração (ICs)			 Descobrir inventário de software e hardware	<p>A Descoberta do ITOM identifica e adiciona itens de configuração de hardware e software ao CMDB, incluindo aplicações de negócios e serviços de aplicações.</p> <p>A Descoberta fornece um inventário atualizado de software e hardware. Usando o APM, obtenha visibilidade completa do seu inventário de aplicações.</p>

Tradução automática

Funcionalidade	Espaço do AE	ITAM	ITOM	Todas as aplicações juntas
Mapeamento de serviços			 Mapear infraestrutura para capacidade de negócios.	<p>O Mapeamento de serviços fornece os relacionamentos entre uma instância da aplicação e a infraestrutura descoberta. O Mapeamento de serviços cria dependências de contexto de serviço de negócio nos ICs descobertos que oferecem suporte à aplicação (instâncias de aplicação ou serviços de aplicações para ambientes de produção, desenvolvimento e teste).</p>
Conteúdo de ciclo de vida de modelos de produto de software e hardware padronizados				<p>A Software Asset Management (SAM) cria um inventário normalizado dos modelos de software que oferecem suporte a um serviço de aplicativos. A Gestão de portfólio de tecnologias (TPM) dos APMs usa o inventário de software SAM para gerenciar os ciclos de vida do fornecedor.</p> <p>Como parte do APM, a capacidade de Gestão de portfólio de tecnologias utiliza dados de ciclo de vida de software e hardware do SAM/HAM para identificar proativamente quais aplicações</p>

Tradução automática

Funcionalidade	Espaço do AE	ITAM	ITOM	Todas as aplicações juntas
				de negócios estão em risco técnico por dependerem de software e hardware sem suporte ou em fim de vida útil.

- O APM aproveita essa capacidade para fornecer visibilidade sobre os riscos associados a uma aplicação de negócios (por exemplo, perda de disponibilidade e o acompanhamento dos controles aplicados para testar a conformidade da aplicação com as regulamentações).
 - O monitoramento contínuo da conformidade garante que essas aplicações sejam certificadas em relação aos controles corretos. Dessa forma, podemos garantir a resiliência operacional das aplicações de negócios. - Com a frequência e os níveis de severidade de ataque continuando a aumentar, as organizações podem ficar sobrecarregadas com o volume de alertas de segurança e achar difícil priorizar e resolver ameaças rapidamente.

Fluxo de trabalho de Espaço de arquitetura empresarial

Use Espaço de arquitetura empresarial e Gestão de ativos de TI e IT Operations Management juntos para obter estes benefícios:

- Permita que os Arquitetos empresariais automatizem o acompanhamento de versões e ciclos de vida de tecnologias subjacentes e determinem quais aplicações de negócios estão em risco devido a tecnologias expiradas ou em fim de vida útil.
- Maior visibilidade do inventário de aplicações. Descubra aplicações redundantes e obsoletas e tome decisões rápidas de acordo.
- Conduza fluxos de trabalho acionáveis para impedir gastos excessivos com licenças que não estão mais sendo usadas.

Requisitos para Espaço de arquitetura empresarial, Gestão de ativos de TI e IT Operations Management

- Instale a aplicação Espaço de arquitetura empresarial (sn_apm_ws).
- Instale a aplicação Gestão de portfólio de tecnologias (sn_apm_tpm).
- Instale a aplicação Software Asset Management Professional (com.sn_samp_master).
- Instale a aplicação Gestão de ativos de hardware (com.sn_hamp).

Introdução à avaliação de riscos de tecnologia para sua empresa

Para começar a avaliar seus riscos de tecnologia, siga estas etapas:

1. Alinhe as tecnologias de suas aplicações de negócios com suas iniciativas de negócios estratégicas. Você pode executar um trabalho agendado para buscar os dados do ciclo de vida da tecnologia para o seu portfólio de tecnologias. Consulte [Run a scheduled job to generate TPM lifecycle data](#).
2. Exiba o risco do ciclo de vida da tecnologia para aplicações de negócios, serviços de aplicações, servidores, produtos de software e modelos de hardware na guia **Portfólio de tecnologias** na seção Informações de Espaço do AE. Você pode filtrar esses riscos de ciclo

de vida de tecnologia para ver somente a aplicação em que está interessado. Consulte [Viewing insights of your portfolio](#) .

3. Rastreie o andamento da análise Gestão de portfólio de tecnologias (TPM) examinando a tabela Log de execução de tecnologia descoberta de TPM [sn_apm_tpm_discovered_tecnologia_run_log]. Cada vez que a análise é executada, uma entrada é adicionada a esta tabela. Para ver os logs de execução, no Espaço do AE, navegue até **Portfólio** Exibição de lista (Espaço do EA > Portfólio > Gestão de portfólio de tecnologias > Logs). Consulte [Portfolio list view](#) .
4. Racionalize suas aplicações de negócios para analisar aplicações de negócios com base em várias pontuações, criar uma demanda para uma aplicação de negócios, definir a disposição planejada de uma aplicação de negócios e adicionar detalhes do ciclo de vida a uma aplicação de negócios existente. Consulte [Rationalization of business applications](#) .

[End]