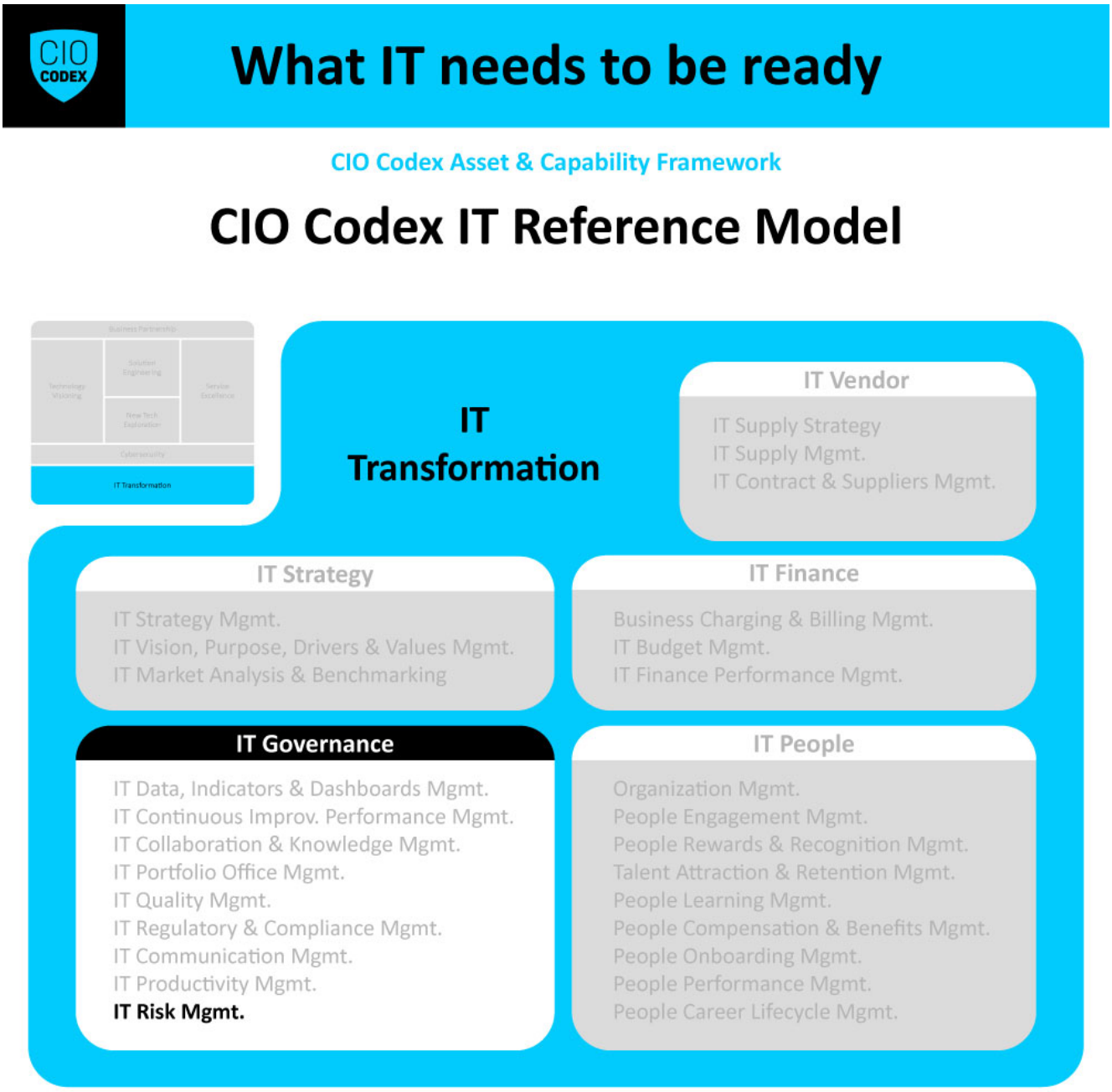

A IT Risk Management, inserida na macro capability IT Governance e parte integrante da camada IT Transformation do CIO Codex Capability Framework, representa um papel vital na proteção dos ativos de TI e na garantia da continuidade dos serviços dentro das organizações.

Esta capability, através de uma abordagem proativa e baseada em dados, permite à organização enfrentar incertezas e tomar decisões informadas para evitar impactos adversos.

Sua relevância é inquestionável para a manutenção da resiliência da TI e para o sucesso dos negócios em um ambiente em constante evolução e desafios tecnológicos.

Esta capability fundamenta-se em conceitos cruciais, como a Identificação de Riscos, a Análise de Riscos, a Mitigação de Riscos, a Resiliência e o Monitoramento Contínuo.

A Identificação de Riscos envolve o reconhecimento e catalogação de possíveis eventos ou condições que possam afetar negativamente as operações de TI.

A Análise de Riscos assessora a probabilidade e o impacto dos riscos identificados, enquanto a Mitigação de Riscos abrange o desenvolvimento e implementação de estratégias para minimizar a probabilidade de ocorrência e/ou o impacto destes riscos.

A Resiliência foca na capacidade organizacional de adaptação e recuperação eficaz frente a eventos de risco, minimizando as interrupções.

O Monitoramento Contínuo garante que as estratégias de mitigação permaneçam eficazes ao longo do tempo.

Características essenciais da IT Risk Management incluem a Avaliação Holística de Riscos, Políticas de Riscos, Planos de Contingência, Testes de Riscos e Comunicação de Riscos.

Estas características são fundamentais para garantir uma abordagem consistente e eficaz na gestão de riscos, estabelecendo políticas claras, desenvolvendo planos para situações emergenciais, realizando testes regulares e mantendo uma comunicação eficiente sobre os riscos identificados.

O propósito central desta capability é assegurar que as ameaças sejam identificadas e tratadas de forma proativa, minimizando o impacto negativo nas operações de TI e na organização como um todo.

Seus objetivos abrangem a identificação e avaliação de riscos de TI, a mitigação de riscos, o monitoramento e relatório de riscos, e a integração da gestão de riscos com a gestão de riscos corporativos.

A IT Risk Management impacta várias dimensões tecnológicas: na Infraestrutura, influencia a seleção de recursos de segurança, na Arquitetura, define padrões que incorporam medidas de segurança e resiliência, nos Sistemas, implica na implementação de sistemas de monitoramento de segurança e políticas de acesso, no Modelo Operacional, estabelece processos de gerenciamento de incidentes e práticas de resposta, e em Cybersecurity, avalia e prioriza ameaças para uma alocação eficaz de recursos de segurança.

Em suma, a IT Risk Management é uma capability essencial que permeia todas as atividades de TI, fornecendo a base para uma operação segura e eficiente.

Ela não apenas protege a organização contra riscos e ameaças, mas também contribui

significativamente para a sustentabilidade e o sucesso contínuo da organização no dinâmico ambiente de negócios de hoje.

A implementação e manutenção efetivas desta capability são, portanto, fundamentais para o gerenciamento eficaz de riscos e para a promoção de uma cultura organizacional resiliente e adaptável.

Conceitos e Características

A IT Risk Management desempenha um papel vital na proteção dos ativos de TI e na garantia da continuidade dos serviços.

Sua abordagem proativa e baseada em dados ajuda a organização a enfrentar incertezas e a tomar decisões informadas para evitar impactos adversos.

Essa capability é essencial para manter a resiliência da TI e o sucesso dos negócios em um ambiente em constante evolução.

Conceitos

- Identificação de Riscos: O processo de reconhecimento e catalogação de possíveis eventos ou condições que podem afetar negativamente as operações de TI.
- Análise de Riscos: Envolve a avaliação da probabilidade e do impacto dos riscos identificados, visando priorizar as ações de mitigação.
- Mitigação de Riscos: Compreende o desenvolvimento e a implementação de estratégias e controles para reduzir a probabilidade de ocorrência e/ou o impacto dos riscos.
- Resiliência: Refere-se à capacidade da organização de se adaptar e se recuperar de eventos de risco de maneira eficaz, minimizando interrupções nos serviços de TI.
- Monitoramento Contínuo: O acompanhamento constante dos riscos, garantindo que as estratégias de mitigação permaneçam eficazes ao longo do tempo.

Características

- Avaliação Holística de Riscos: Realiza uma avaliação abrangente dos riscos que afetam a TI, considerando aspectos técnicos, operacionais e estratégicos.
- Políticas de Riscos: Estabelece políticas e diretrizes claras para a gestão de riscos, garantindo uma abordagem consistente em toda a organização.
- Planos de Contingência: Desenvolve planos de contingência para situações de emergência, assegurando a continuidade das operações em caso de eventos adversos.
- Testes de Riscos: Realiza testes e simulações regulares para validar a eficácia dos planos de mitigação de riscos.
- Comunicação de Riscos: Mantém um canal de comunicação aberto com as partes interessadas, informando sobre os riscos identificados e as medidas de mitigação adotadas.

Propósito e Objetivos

A IT Risk Management desempenha um papel fundamental na governança de TI, concentrando-se na identificação, análise e mitigação de riscos associados às operações de Tecnologia da Informação.

Seu propósito central é assegurar que as ameaças sejam identificadas e tratadas de forma proativa, minimizando o impacto negativo nas operações de TI e, consequentemente, na organização como um todo.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, os objetivos da IT Risk Management são:

- Identificar Riscos de TI: Realizar uma análise detalhada para identificar os diversos tipos de riscos que podem afetar as operações de TI, tais como riscos de segurança cibernética, riscos operacionais e riscos de conformidade.
- Avaliar a Severidade e Probabilidade: Avaliar a gravidade potencial e a probabilidade de ocorrência de cada risco identificado, atribuindo uma classificação que orienta o tratamento adequado.

- Mitigar Riscos: Desenvolver e implementar estratégias de mitigação de riscos, que podem incluir a definição de controles de segurança, processos de contingência e planos de resposta a incidentes.
- Monitorar e Relatar Riscos: Estabelecer um sistema contínuo de monitoramento de riscos e incidentes, bem como relatórios regulares para a alta administração e partes interessadas.
- Integrar a Gestão de Riscos: Integre a gestão de riscos de TI com a gestão de riscos corporativos, garantindo que os riscos de TI estejam alinhados com os objetivos estratégicos da organização.

Impacto na Tecnologia

A IT Risk Management influencia diversas dimensões da tecnologia:

- Infraestrutura: Influencia a seleção de infraestrutura de segurança, como firewalls, sistemas de detecção de intrusão e sistemas de prevenção de ameaças, para mitigar os riscos de segurança cibernética.
- Arquitetura: Define padrões de arquitetura que incorporam medidas de segurança e resiliência para proteger a infraestrutura contra ameaças e vulnerabilidades.
- Sistemas: Inclui a implementação de sistemas de monitoramento de segurança e a definição de políticas de acesso para proteger os sistemas contra ameaças internas e externas.
- Modelo Operacional: Define processos de gerenciamento de incidentes, planos de continuidade de negócios e práticas de resposta a incidentes para manter a continuidade das operações de TI em caso de ameaças.
- Cybersecurity: A gestão de riscos avalia e prioriza ameaças, permitindo a alocação eficaz de recursos de segurança.

Roadmap de Implementação

A capability de IT Risk Management, inserida na macro capability de IT Governance e na camada de IT Transformation, desempenha um papel crucial na proteção dos ativos de TI e na garantia da continuidade dos serviços.

A abordagem proativa e baseada em dados dessa capability ajuda as organizações a enfrentarem incertezas e a tomarem decisões informadas para evitar impactos adversos.

Neste contexto, o roadmap de implementação da IT Risk Management, fornecendo orientações sobre como planejar e executar a adoção dessa capability, incluindo fatores críticos de sucesso e etapas essenciais:

- Avaliação Inicial de Riscos: Inicie o processo de implementação realizando uma avaliação abrangente dos riscos que afetam a TI. Isso envolve a identificação de possíveis eventos ou condições que podem prejudicar as operações de TI. Crie um inventário de riscos, classificando-os com base na gravidade e na probabilidade de ocorrência.
- Definição de Objetivos e Estratégias: Estabeleça objetivos claros para a gestão de riscos de TI, alinhados com os objetivos estratégicos da organização. Desenvolva estratégias para mitigar os riscos identificados, considerando medidas preventivas e planos de contingência.
- Políticas e Diretrizes de Riscos: Estabeleça políticas e diretrizes claras para a gestão de riscos, garantindo uma abordagem consistente em toda a organização. Comunique essas políticas a todas as partes interessadas e equipe de TI.
- Implementação de Controles de Riscos: Desenvolva e implemente controles internos e medidas de segurança para reduzir a probabilidade de ocorrência e/ou o impacto dos riscos. Isso pode incluir a implementação de tecnologias de segurança cibernética, a definição de políticas de acesso e a adoção de melhores práticas.
- Testes e Simulações de Riscos: Realize testes e simulações regulares para validar a eficácia dos planos de mitigação de riscos. Avalie a capacidade da equipe de TI em responder a situações de risco simuladas.
- Monitoramento Contínuo: Estabeleça um sistema de monitoramento contínuo de riscos e incidentes de segurança. Utilize ferramentas de monitoramento de segurança e crie métricas para avaliar a eficácia das estratégias de mitigação.
- Comunicação de Riscos: Mantenha um canal de comunicação aberto com todas as partes interessadas, informando sobre os riscos identificados e as medidas de mitigação em andamento. Isso promove a transparência e a colaboração na gestão de riscos.

- Integração com a Governança Corporativa: Integre a gestão de riscos de TI com a governança corporativa, garantindo que os riscos de TI estejam alinhados com os objetivos estratégicos da organização. Colabore com outras áreas, como auditoria interna e compliance, para garantir a conformidade global.
- Avaliação e Aprimoramento Constantes: Realize avaliações regulares da eficácia das estratégias de mitigação e das políticas de riscos. Ajuste as medidas de acordo com as mudanças no cenário de riscos e as lições aprendidas com incidentes passados.

A implementação bem-sucedida da IT Risk Management é fundamental para garantir a resiliência da TI e o sucesso dos negócios em um ambiente dinâmico e desafiador.

Ao seguir este roadmap, as organizações podem fortalecer sua capacidade de identificar, analisar e mitigar riscos de TI, protegendo assim seus ativos e garantindo a continuidade dos serviços críticos.

Melhores Práticas de Mercado

A IT Risk Management, no contexto do CIO Codex Capability Framework, desempenha um papel fundamental na proteção dos ativos de TI e na garantia da continuidade dos serviços.

As melhores práticas de mercado nesta área são cruciais para enfrentar incertezas e tomar decisões informadas.

A seguir, as principais melhores práticas de mercado:

- Avaliação Holística de Riscos: Realizar uma avaliação abrangente dos riscos que afetam a TI, considerando aspectos técnicos, operacionais e estratégicos. Isso garante que todos os tipos de riscos sejam identificados e gerenciados de forma adequada.
- Políticas de Riscos Claras: Estabelecer políticas e diretrizes claras para a gestão de riscos, garantindo uma abordagem consistente em toda a organização. Isso inclui a definição de papéis e responsabilidades.
- Planos de Contingência Efetivos: Desenvolver planos de contingência detalhados para situações de emergência, assegurando a continuidade

das operações em caso de eventos adversos. Testar regularmente esses planos para garantir sua eficácia.

- Monitoramento Contínuo de Riscos: Implementar um sistema de monitoramento contínuo de riscos, permitindo a identificação precoce de ameaças e a adaptação ágil das estratégias de mitigação.
- Integração com a Gestão de Riscos Corporativos: Integrar a gestão de riscos de TI com a gestão de riscos corporativos para garantir que os riscos de TI estejam alinhados com os objetivos estratégicos da organização.
- Identificação Proativa de Riscos de TI: Realizar análises detalhadas para identificar diversos tipos de riscos que podem afetar as operações de TI, como riscos de segurança cibernética, riscos operacionais e riscos de conformidade.
- Avaliação de Severidade e Probabilidade: Avaliar a gravidade potencial e a probabilidade de ocorrência de cada risco identificado, atribuindo classificações que orientam o tratamento adequado.
- Estratégias de Mitigação Eficazes: Desenvolver e implementar estratégias de mitigação de riscos, incluindo a definição de controles de segurança, processos de contingência e planos de resposta a incidentes.
- Comunicação Transparente de Riscos: Manter um canal de comunicação aberto com as partes interessadas, informando sobre os riscos identificados e as medidas de mitigação adotadas. Isso promove a transparência e a confiança.
- Avaliação de Fornecedores: Avaliar regularmente fornecedores e parceiros de TI quanto aos riscos que podem representar para a organização. Isso inclui avaliar a segurança de terceiros.
- Treinamento e Conscientização: Oferecer treinamento regular para a equipe de TI sobre as políticas e procedimentos de gerenciamento de riscos, garantindo que todos compreendam seu papel na mitigação de riscos.

A implementação dessas melhores práticas de mercado na capability de IT Risk Management é crucial para garantir a resiliência da TI, minimizar o impacto de eventos adversos e proteger os interesses da organização.

Elas fornecem uma estrutura sólida para identificar, avaliar e mitigar riscos, contribuindo para o sucesso contínuo dos negócios em um ambiente em constante evolução.

Desafios Atuais

A IT Risk Management desempenha um papel fundamental na governança de TI, concentrando-se na identificação, análise e mitigação de riscos associados às operações de Tecnologia da Informação.

No entanto, ao adotar e integrar essa capability em seus processos de negócios e operações de TI, as organizações se deparam com uma série de desafios atuais, baseados nas melhores práticas do mercado.

A seguir, destacam-se os principais desafios enfrentados pelas organizações no contexto do CIO Codex Capability Framework:

- Crescente Complexidade Tecnológica: O ambiente de TI está se tornando cada vez mais complexo, com a proliferação de tecnologias emergentes, como inteligência artificial e Internet das Coisas (IoT), o que torna a identificação e mitigação de riscos mais desafiadoras.
- Riscos Cibernéticos em Evolução: As ameaças cibernéticas estão em constante evolução, com atacantes desenvolvendo táticas mais sofisticadas. Manter-se à frente dessas ameaças requer uma abordagem ágil e proativa.
- Conformidade com Regulamentações: O cumprimento de regulamentações, como GDPR e LGPD, é um desafio contínuo, especialmente no que diz respeito à proteção de dados pessoais e privacidade.
- Integração de Riscos Corporativos: Integrar a gestão de riscos de TI com a gestão de riscos corporativos é complexo, mas essencial para alinhar os objetivos estratégicos da organização.
- Avaliação de Terceiros: Avaliar e mitigar riscos associados a fornecedores e parceiros terceirizados requer um processo rigoroso de due diligence.
- Volume Crescente de Dados: O aumento exponencial no volume de dados torna desafiador o monitoramento e a proteção contra vazamentos de informações sensíveis.
- Escassez de Profissionais de Segurança: A falta de profissionais qualificados em segurança cibernética dificulta a construção e a manutenção de equipes de gerenciamento de riscos eficazes.

- Resposta a Incidentes: Desenvolver planos de resposta a incidentes eficazes e testá-los regularmente é um desafio, especialmente com a variedade de ameaças potenciais.
- Conscientização Organizacional: Criar uma cultura de conscientização sobre segurança e riscos em toda a organização exige esforços contínuos de treinamento e comunicação.
- Pressões Orçamentárias: Equilibrar a necessidade de investimentos em segurança com restrições orçamentárias é um desafio constante para muitas organizações.

Enfrentar esses desafios é crucial para garantir que a IT Risk Management alcance seus objetivos de identificar, avaliar e mitigar riscos de maneira eficaz.

Isso requer um compromisso contínuo com a atualização das práticas de segurança cibernética, a conformidade regulatória e o desenvolvimento de estratégias de mitigação adaptáveis às ameaças em evolução.

Além disso, a integração eficaz da gestão de riscos de TI com a gestão de riscos corporativos é fundamental para garantir que os riscos estejam alinhados com os objetivos estratégicos da organização.

O sucesso nessa área não apenas protege os ativos de TI, mas também contribui para a continuidade dos serviços e a resiliência da organização em um ambiente de negócios dinâmico e repleto de desafios.

Tendências para o Futuro

A IT Risk Management desempenha um papel crítico na proteção dos ativos de TI e na manutenção da continuidade dos serviços em um ambiente constantemente mutável.

Para entender como essa capability evoluirá no futuro e se adaptará às demandas em evolução, é essencial considerar as tendências emergentes e as expectativas do mercado.

Abaixo, as principais tendências futuras dentro do contexto do CIO Codex Capability Framework:

- Inteligência Artificial na Análise de Riscos: A utilização de algoritmos de IA para analisar dados e identificar potenciais riscos se tornará mais

prevalente, permitindo uma detecção mais rápida e precisa de ameaças.

- Análise Preditiva de Riscos: A capacidade de prever riscos com base em dados históricos e padrões emergentes permitirá a tomada de decisões proativas para mitigação de riscos.
- Cibersegurança Avançada: A crescente sofisticação das ameaças cibernéticas exigirá abordagens de segurança igualmente avançadas, com foco na detecção e resposta em tempo real.
- Gestão de Riscos de Terceiros: Com a terceirização cada vez mais comum, a gestão de riscos relacionados a parceiros e fornecedores se tornará uma prioridade, com a necessidade de avaliar e mitigar riscos em toda a cadeia de suprimentos.
- Conformidade Regulatória em Tempo Real: As organizações buscarão sistemas que permitam o monitoramento contínuo da conformidade regulatória, garantindo que estejam em conformidade em todos os momentos.
- Análise de Riscos de Privacidade de Dados: Com a crescente regulamentação da privacidade de dados, a análise de riscos relacionados à proteção de informações pessoais será fundamental.
- Riscos Ambientais e Sustentabilidade: A consideração dos riscos ambientais e a incorporação de práticas sustentáveis na gestão de riscos se tornarão mais proeminentes, alinhando-se às preocupações globais com a sustentabilidade.
- Blockchain para Registro de Riscos: A tecnologia blockchain será empregada para criar registros imutáveis de riscos e mitigação, aumentando a transparência e a confiabilidade.
- Integração com Inteligência de Negócios (BI): A integração de dados de gestão de riscos com soluções de BI permitirá análises mais profundas e relatórios mais abrangentes para apoiar a tomada de decisões estratégicas.
- Educação em Gestão de Riscos: A conscientização e a educação em gestão de riscos se tornarão uma prioridade, capacitando os funcionários a identificarem e relatar riscos em suas áreas de atuação.

Essas tendências refletem a natureza dinâmica da IT Risk Management, que continuará a se adaptar às mudanças no ambiente de negócios e nas ameaças emergentes.

À medida que a tecnologia e as práticas comerciais evoluem, a capacidade de

antecipar e responder a riscos se tornará ainda mais crucial para garantir a resiliência das operações de TI e o sucesso global da organização.

KPIs Usuais

A capability IT Risk Management desempenha um papel crucial na proteção dos ativos de TI e na garantia da continuidade dos serviços em um cenário de constante evolução e incertezas.

Para avaliar adequadamente o desempenho desta capability, é fundamental acompanhar indicadores-chave de desempenho (KPIs) relevantes que demonstrem a capacidade de identificar, analisar e mitigar riscos associados às operações de Tecnologia da Informação.

Abaixo, uma lista dos principais KPIs usuais usados no mercado, considerando o contexto do CIO Codex Capability Framework:

- Taxa de Identificação de Riscos: Mede a eficácia do processo de reconhecimento e catalogação de eventos ou condições que podem afetar negativamente as operações de TI.
- Taxa de Análise de Riscos: Avalia a capacidade de avaliar a probabilidade e o impacto dos riscos identificados, priorizando ações de mitigação com base em análises sólidas.
- Taxa de Mitigação de Riscos: Calcula o progresso na implementação de estratégias e controles para reduzir a probabilidade de ocorrência e/ou o impacto dos riscos identificados.
- Taxa de Resiliência: Mede a capacidade da organização de se adaptar e se recuperar eficazmente de eventos de risco, minimizando interrupções nos serviços de TI.
- Taxa de Monitoramento Contínuo: Avalia a eficiência do acompanhamento constante dos riscos, garantindo que as estratégias de mitigação permaneçam eficazes ao longo do tempo.
- Taxa de Identificação de Riscos de Segurança Cibernética: Mede a capacidade de identificar e avaliar os riscos específicos de segurança cibernética que podem afetar a TI.
- Taxa de Resposta a Incidentes de Segurança: Avalia a eficácia da resposta

a incidentes de segurança cibernética, incluindo o tempo de resposta e a eficácia das medidas tomadas.

- Taxa de Atualização de Políticas de Riscos: Mede a frequência com que as políticas e diretrizes para a gestão de riscos são atualizadas para refletir as mudanças nas ameaças e vulnerabilidades.
- Taxa de Testes de Riscos: Avalia a frequência com que são realizados testes e simulações para validar a eficácia dos planos de mitigação de riscos.
- Taxa de Comunicação de Riscos: Mede a eficiência da comunicação de riscos identificados para as partes interessadas internas e externas, incluindo relatórios regulares.
- Taxa de Alinhamento com Objetivos Estratégicos: Avalia o grau de alinhamento das atividades de gestão de riscos de TI com os objetivos estratégicos da organização.
- Taxa de Cumprimento de Regulamentações: Calcula o grau de conformidade com as regulamentações específicas que se aplicam às operações de TI.
- Taxa de Implementação de Planos de Contingência: Mede o progresso na implementação de planos de contingência para situações de emergência.
- Taxa de Avaliação de Impacto de Novas Ameaças: Avalia a rapidez com que a TI avalia o impacto de novas ameaças e vulnerabilidades em suas operações.
- Taxa de Integração da Gestão de Riscos: Mede o grau de integração da gestão de riscos de TI com a gestão de riscos corporativos, garantindo uma abordagem alinhada com os objetivos estratégicos.

Esses KPIs são fundamentais para avaliar o desempenho da IT Risk Management, garantindo que ela atinja seus objetivos de identificar, analisar e mitigar riscos associados às operações de TI de forma eficaz.

Eles também contribuem para a proteção dos ativos de TI e a manutenção da continuidade dos serviços em um ambiente em constante evolução e desafios.

Exemplos de OKRs

A capability de IT Risk Management desempenha um papel fundamental na identificação, análise e mitigação de riscos associados às operações de TI.

Abaixo, exemplos de Objetivos e Resultados-Chave (OKRs) relacionados a essa capability:

Identificação de Riscos de TI

Objetivo: Identificar de forma abrangente todos os riscos associados às operações de TI.

- KR1: Realizar uma análise detalhada das operações de TI para identificar possíveis fontes de risco.
- KR2: Desenvolver um registro de riscos de TI que inclua todas as ameaças identificadas.
- KR3: Classificar os riscos de acordo com sua gravidade e probabilidade de ocorrência.

Análise de Riscos

Objetivo: Analisar em profundidade os riscos identificados para compreender seu impacto potencial.

- KR1: Realizar avaliações de risco detalhadas para cada ameaça identificada.
- KR2: Avaliar o impacto financeiro, operacional e reputacional de cada risco.
- KR3: Determinar a probabilidade de ocorrência de cada risco.

Mitigação de Riscos

Objetivo: Desenvolver estratégias eficazes de mitigação de riscos para reduzir a exposição da organização.

- KR1: Desenvolver planos de mitigação específicos para cada risco identificado.

- KR2: Implementar controles e medidas de segurança para reduzir a probabilidade e o impacto dos riscos.
- KR3: Estabelecer responsabilidades claras para a execução dos planos de mitigação.

Monitoramento Contínuo de Riscos

Objetivo: Manter um monitoramento constante dos riscos de TI e ajustar as estratégias de mitigação conforme necessário.

- KR1: Implementar um sistema de monitoramento em tempo real para identificar mudanças nos riscos.
- KR2: Realizar revisões regulares dos planos de mitigação e ajustá-los com base nas mudanças nos riscos.
- KR3: Criar um processo de relatórios de riscos que comunique proativamente as atualizações aos stakeholders relevantes.

Cultura de Conscientização de Riscos

Objetivo: Promover uma cultura de conscientização de riscos dentro da equipe de TI e em toda a organização.

- KR1: Realizar treinamentos regulares sobre gerenciamento de riscos para sensibilizar a equipe.
- KR2: Estabelecer políticas claras de gerenciamento de riscos e comunicá-las de maneira eficaz.
- KR3: Reconhecer e premiar ações que demonstrem uma abordagem proativa para o gerenciamento de riscos.

Resposta a Incidentes de Segurança

Objetivo: Ter planos de resposta eficazes para incidentes de segurança relacionados a riscos de TI.

- KR1: Desenvolver planos de resposta a incidentes que abordem cenários de riscos específicos.
- KR2: Treinar a equipe de TI na execução dos planos de resposta a

incidentes.
- KR3: Realizar exercícios de simulação de incidentes para testar a eficácia dos planos.

Esses OKRs são essenciais para a capability de IT Risk Management, pois garantem que os riscos associados às operações de TI sejam identificados, analisados e mitigados de forma eficaz.

Além disso, promovem uma cultura de conscientização de riscos e garantem que a organização esteja preparada para responder a incidentes de segurança relacionados a riscos de TI.

Critérios para Avaliação de Maturidade

A capability IT Risk Management, inserida na macro capability IT Governance e na camada IT Transformation, é de vital importância para a identificação, análise e mitigação de riscos associados às operações de TI.

Esta capability desempenha um papel crucial na gestão proativa de riscos, assegurando que as ameaças sejam identificadas e tratadas de forma a minimizar o impacto negativo nas operações de TI e na organização como um todo.

A avaliação de maturidade na IT Risk Management é fundamental para garantir que a organização tenha um controle eficaz sobre os riscos de TI.

Seguindo o modelo inspirado no CMMI, foram definidos cinco níveis de maturidade: Inexistente, Inicial, Definido, Gerenciado e Otimizado:

Nível de Maturidade Inexistente

- Não há reconhecimento da necessidade de gerenciamento de riscos de TI na organização.
- Não existem processos ou metodologias para identificar ou avaliar riscos de TI.
- Não são atribuídas responsabilidades específicas para o gerenciamento de riscos de TI.
- Não há monitoramento ou acompanhamento de incidentes relacionados a

riscos de TI.
- A organização não possui um registro de riscos de TI identificados.

Nível de Maturidade Inicial

- A organização reconhece a importância do gerenciamento de riscos de TI, mas de forma limitada.
- Processos iniciais para identificar e avaliar riscos de TI estão sendo desenvolvidos.
- Responsabilidades iniciais são designadas para funções específicas no gerenciamento de riscos de TI.
- Incidentes relacionados a riscos de TI são registrados, mas a análise é ad hoc.
- Um registro inicial de riscos de TI é mantido, mas não está completamente estruturado.

Nível de Maturidade Definido

- A organização possui políticas e procedimentos documentados para o gerenciamento de riscos de TI.
- Processos estruturados são utilizados para identificar, avaliar e classificar riscos de TI.
- Responsabilidades claras e atribuições são definidas para funções de gerenciamento de riscos de TI.
- Incidentes relacionados a riscos de TI são registrados e analisados sistematicamente.
- Um registro abrangente de riscos de TI é mantido, incluindo informações sobre probabilidade e impacto.

Nível de Maturidade Gerenciado

- O gerenciamento de riscos de TI é parte integrante da cultura organizacional.
- Processos avançados e automatizados são usados para identificar, avaliar

e classificar riscos de TI.
- Monitoramento contínuo de incidentes relacionados a riscos de TI é realizado.
- Controles sofisticados são implementados para mitigar riscos identificados.
- A organização mantém um registro de riscos de TI altamente detalhado e atualizado em tempo real.

Nível de Maturidade Otimizado

- A gestão de riscos de TI é uma prática de classe mundial na organização.
- Processos de gerenciamento de riscos de TI são altamente eficazes e otimizados.
- A organização utiliza análises avançadas para prever riscos futuros.
- Controles são constantemente aprimorados e automatizados.
- A organização mantém uma abordagem proativa para a gestão de riscos de TI, visando a resiliência organizacional.

A avaliação de maturidade na capability IT Risk Management é essencial para garantir que a organização esteja adequadamente preparada para identificar, analisar e mitigar riscos de TI.

À medida que a maturidade aumenta, a organização se torna mais capaz de enfrentar desafios e ameaças, contribuindo para a resiliência e o sucesso a longo prazo.

Convergência com Frameworks de Mercado

A capability IT Risk Management, enquadrada na macro capability IT Governance e na camada IT Transformation, é fundamental para o processo de identificação, análise e mitigação dos riscos associados às operações de TI.

Esta capability desempenha um papel crucial na gestão proativa de riscos, assegurando que as ameaças sejam identificadas e tratadas adequadamente para minimizar impactos negativos nas operações de TI e na organização como um todo.

A seguir, é analisada a convergência desta capability em relação a um conjunto dez frameworks de mercado reconhecidos e bem estabelecidos em suas respectivas áreas de expertise:

COBIT

- Nível de Convergência: Alto
- Racional: O COBIT proporciona um framework robusto para a governança de TI, onde a gestão de riscos é um elemento central. Este framework enfatiza a importância de identificar, avaliar e gerir riscos de TI, garantindo uma alta convergência com a capability "IT Risk Management".

ITIL

- Nível de Convergência: Médio
- Racional: O ITIL, focado na gestão de serviços de TI, aborda a gestão de riscos principalmente no contexto de entrega de serviços. Embora não seja o foco principal, a mitigação de riscos é reconhecida como um aspecto importante na garantia de serviços de TI eficientes e confiáveis.

SAFe

- Nível de Convergência: Baixo
- Racional: O SAFe, como um framework ágil, concentra-se mais na entrega rápida e adaptativa de valor. Embora reconheça a importância da gestão de riscos, sua abordagem é mais focada no nível de projeto e desenvolvimento de produto, e não tanto em um contexto abrangente de TI.

PMI

- Nível de Convergência: Médio
- Racional: O PMI, com seu enfoque em gerenciamento de projetos, inclui a

gestão de riscos como um aspecto fundamental. No entanto, seu foco está mais em riscos de projeto do que em riscos operacionais de TI de uma perspectiva mais ampla.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI incorpora a gestão de riscos como parte da melhoria de processos. Contudo, seu foco está mais na qualidade e eficiência dos processos do que na gestão abrangente de riscos de TI.

TOGAF

- Nível de Convergência: Baixo
- Racional: O TOGAF, focado em arquitetura empresarial, aborda a gestão de riscos em um contexto mais estratégico e de design. A gestão de riscos operacionais de TI é menos enfatizada neste framework.

DevOps SRE

- Nível de Convergência: Baixo
- Racional: O DevOps SRE prioriza a confiabilidade e a entrega contínua, com menos ênfase em aspectos formais de gestão de riscos. Embora a mitigação de riscos seja intrínseca ao processo, não é um foco direto deste framework.

NIST

- Nível de Convergência: Alto
- Racional: O NIST, especialmente com seus frameworks de segurança cibernética, tem forte alinhamento com a gestão de riscos de TI. Seu enfoque em segurança e conformidade ressoa diretamente com os objetivos da capability “IT Risk Management”.

Six Sigma

- Nível de Convergência: Médio
- Racional: O Six Sigma, com seu foco em melhoria de processos e redução de defeitos, aborda indiretamente a gestão de riscos ao melhorar a eficiência e a qualidade dos processos de TI.

Lean IT

- Nível de Convergência: Baixo
- Racional: Lean IT foca na eficiência operacional e na redução de desperdícios. Enquanto a gestão de riscos pode ser considerada no contexto de eficiência operacional, não é um foco principal deste framework.

A IT Risk Management é, portanto, um elemento vital na governança de TI, interagindo de diversas maneiras com diferentes frameworks de mercado.

Sua capacidade de identificar e mitigar riscos ajuda a garantir a resiliência e a eficácia das operações de TI, protegendo a organização contra uma variedade de ameaças internas e externas.

A integração desta capability com frameworks como COBIT e NIST demonstra seu papel essencial na estruturação de uma abordagem de governança de TI focada na segurança, conformidade e gerenciamento de riscos.

Processos e Atividades

Develop Risk Management Strategy

Desenvolver uma estratégia de gestão de riscos para TI alinhada com os objetivos do negócio é fundamental para identificar, analisar e mitigar os riscos que possam impactar as operações de TI.

Este processo envolve a definição de uma abordagem sistemática para identificar

ameaças potenciais, avaliar suas probabilidades e impactos, e implementar controles eficazes.

A estratégia deve considerar as melhores práticas de mercado e estar alinhada com a estratégia corporativa, garantindo que os riscos de TI sejam gerenciados de maneira integrada.

A comunicação da estratégia para todas as partes interessadas é crucial para assegurar o engajamento e a adesão aos processos de gestão de riscos estabelecidos.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Assess Risk Landscape	Avaliar o panorama de riscos relevantes para a organização.	Informações de risco, benchmarks	Relatório de avaliação de riscos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
2	Define Risk Objectives	Definir os objetivos de gestão de riscos alinhados com os objetivos do negócio.	Feedback de stakeholders, análise de riscos	Objetivos de gestão de riscos definidos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

3	Develop Risk Policies	Desenvolver políticas de gestão de riscos detalhadas e alinhadas com os objetivos definidos.	Objetivos de gestão de riscos, benchmark de políticas	Políticas de gestão de riscos desenvolvidas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation
4	Establish Risk Framework	Estabelecer um framework de gestão de riscos que suporte a implementação das políticas.	Políticas de gestão de riscos, frameworks de referência	Framework de gestão de riscos estabelecido	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
5	Communicate Risk Strategy	Comunicar a estratégia de gestão de riscos para todas as partes interessadas.	Framework de gestão de riscos, políticas de gestão de riscos	Estratégia de gestão de riscos comunicada	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

Identify Potential Risks

Identificar os riscos potenciais que possam impactar a organização é um processo crítico para assegurar que todas as operações de TI estejam preparadas para mitigar ameaças.

Este processo envolve a realização de uma análise detalhada para identificar riscos em várias áreas, como segurança cibernética, operacionais, conformidade e tecnológicos.

A identificação de riscos inclui a coleta de dados através de entrevistas, workshops e revisões de documentação.

A colaboração com diferentes áreas internas e externas é fundamental para garantir uma visão abrangente dos riscos potenciais.

Os riscos identificados devem ser documentados e categorizados para facilitar a análise e priorização subsequente.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Risk Assessments	Realizar avaliações de risco para identificar ameaças potenciais.	Dados de riscos, entrevistas	Relatório de avaliação de riscos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
2	Gather Risk Data	Coletar dados de risco de várias fontes, incluindo entrevistas e workshops.	Informações de risco, dados de entrevistas	Dados de risco coletados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

3	Analyze Risk Data	Analisar os dados coletados para identificar e categorizar riscos potenciais.	Dados de risco coletados	Análise de riscos realizada	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation
4	Document Identified Risks	Documentar os riscos identificados e categorizá-los para priorização.	Análise de riscos realizada	Riscos identificados documentados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
5	Communicate Identified Risks	Comunicar os riscos identificados para as partes interessadas relevantes.	Riscos identificados documentados	Riscos comunicados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

Implement Risk Mitigation Plans

Implementar planos de mitigação de riscos é crucial para minimizar os impactos negativos dos riscos identificados.

Este processo envolve a criação e execução de estratégias para reduzir a probabilidade de ocorrência e/ou o impacto dos riscos.

A implementação deve incluir a designação de responsáveis por cada plano de

mitigação, a criação de processos claros para monitorar a eficácia das ações e a integração de tecnologias que facilitem a mitigação.

Além disso, a comunicação e o treinamento são fundamentais para garantir que todos os colaboradores compreendam suas responsabilidades e estejam preparados para executar os planos de mitigação quando necessário.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Develop Mitigation Plans	Desenvolver planos detalhados de mitigação de riscos para os riscos identificados.	Riscos identificados, políticas de gestão de riscos	Planos de mitigação desenvolvidos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
2	Assign Mitigation Responsibilities	Designar responsáveis por cada aspecto dos planos de mitigação de riscos.	Planos de mitigação desenvolvidos	Responsáveis designados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

3	Implement Mitigation Actions	Implementar as ações de mitigação conforme os planos desenvolvidos.	Planos de mitigação, ferramentas de monitoramento	Ações de mitigação implementadas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation
4	Monitor Mitigation Effectiveness	Monitorar a eficácia das ações de mitigação implementadas.	Ações de mitigação implementadas	Relatórios de eficácia de mitigação	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
5	Communicate Mitigation Status	Comunicar o status das ações de mitigação para as partes interessadas.	Relatórios de eficácia de mitigação	Status de mitigação comunicado	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

Monitor Risk Management Performance

Monitorar continuamente o desempenho da gestão de riscos utilizando indicadores-chave de desempenho (KPIs) é essencial para assegurar que as estratégias e ações de mitigação sejam eficazes.

Este processo inclui a coleta e análise de dados de desempenho, a revisão de incidentes de risco e a avaliação contínua dos controles de risco implementados.

O uso de KPIs permite uma avaliação objetiva e mensurável do sucesso das estratégias

de gestão de riscos.

A comunicação dos resultados para as partes interessadas e a revisão periódica dos KPIs garantem que as ações corretivas possam ser tomadas rapidamente para manter a eficácia do programa de gestão de riscos.

- PDCA focus: Check
- Periodicidade: Trimestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Define Risk KPIs	Definir indicadores-chave de desempenho para monitorar a gestão de riscos.	Objetivos de gestão de riscos, benchmarks	KPIs definidos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
2	Collect Risk Data	Coletar dados de desempenho relacionados aos riscos.	Ferramentas de monitoramento, relatórios de riscos	Dados de risco coletados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

3	Analyze Risk Performance	Analisar os dados coletados para avaliar a eficácia da gestão de riscos.	Dados de risco coletados	Análise de desempenho de riscos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation
4	Review Risk Incidents	Revisar incidentes de risco ocorridos e sua gestão.	Dados de risco, relatórios de incidentes	Relatório de revisão de incidentes	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
5	Report Risk Performance	Relatar o desempenho da gestão de riscos para as partes interessadas.	Análise de desempenho de riscos	Relatório de desempenho de riscos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

Review and Improve Risk Management Processes

Revisar e melhorar continuamente os processos de gestão de riscos com base nos resultados obtidos e feedbacks recebidos é essencial para assegurar que a organização se mantenha resiliente frente a novos desafios.

Este processo envolve a análise dos resultados das auditorias, a identificação de oportunidades de melhoria, e a implementação de ajustes necessários nos processos e controles de riscos.

A revisão deve considerar as melhores práticas do mercado e as lições aprendidas de ciclos anteriores para garantir que os processos estejam atualizados e eficazes.

A comunicação das melhorias implementadas é crucial para garantir a adesão e o entendimento por parte de todas as partes interessadas.

- PDCA focus: Act
- Periodicidade: Semestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Evaluate Risk Management Results	Avaliar os resultados da gestão de riscos com base em auditorias e KPIs.	Relatórios de auditoria, KPIs	Relatório de avaliação de riscos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
2	Identify Improvement Areas	Identificar áreas de melhoria nos processos de gestão de riscos.	Relatório de avaliação de riscos	Áreas de melhoria identificadas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

3	Develop Improvement Plan	Desenvolver um plano detalhado para melhorar os processos de gestão de riscos.	Áreas de melhoria identificadas	Plano de melhoria desenvolvido	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation
4	Implement Process Improvements	Implementar as melhorias conforme o plano desenvolvido.	Plano de melhoria desenvolvido	Melhorias implementadas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
5	Communicate Process Updates	Comunicar as atualizações dos processos de gestão de riscos para as partes interessadas.	Melhorias implementadas	Atualizações comunicadas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation