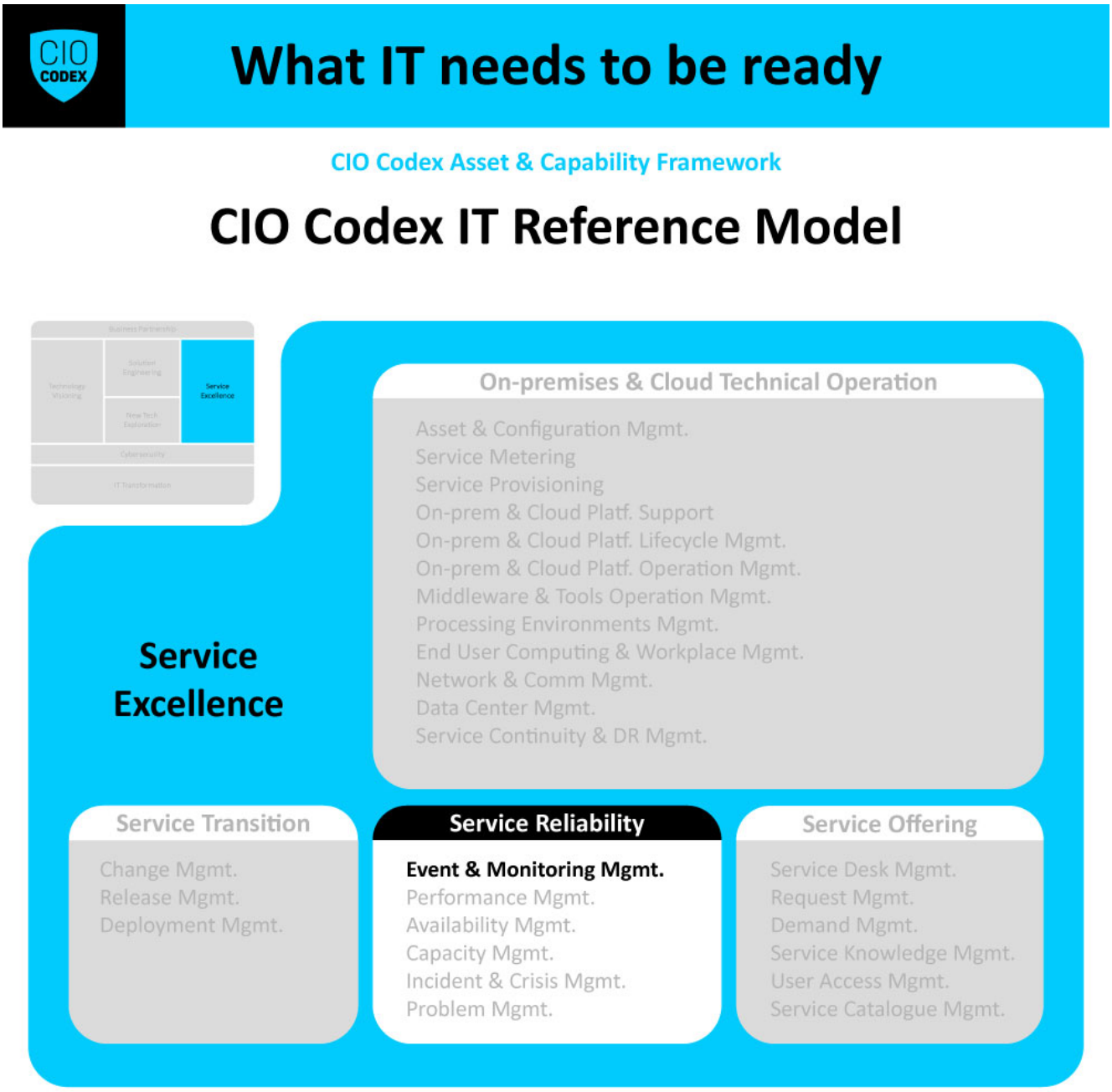

A Event & Monitoring Management, integrante da macro capability Service Reliability na camada Service Excellence do CIO Codex Capability Framework, desempenha um papel crucial na manutenção da qualidade e disponibilidade dos serviços de TI.

Esta capability, com sua abordagem proativa, é fundamental para prevenir problemas, aumentar a eficiência operacional e assegurar uma experiência de usuário contínua e confiável.

Os conceitos-chave associados à Event & Monitoring Management incluem Supervisão Contínua, Eventos de TI e Monitoramento Proativo.

Supervisão Contínua implica na observação constante dos sistemas de TI, coletando

dados para análise.

Eventos de TI referem-se a qualquer ocorrência que possa indicar um problema ou impactar o desempenho.

O Monitoramento Proativo destina-se à identificação e mitigação de problemas antes que estes afetem os serviços.

As características desta capability incluem Alertas e Notificações, Análise de Tendências, Resposta a Eventos, Monitoramento Multifacetado e Integração com outras capabilities, como Incident Management.

Alertas e Notificações são emitidos automaticamente quando eventos críticos ou anomalias são detectados.

A Análise de Tendências examina padrões de longo prazo para identificar riscos e oportunidades de melhoria.

A Resposta a Eventos envolve procedimentos claros para restaurar a normalidade.

O Monitoramento Multifacetado abrange performance, segurança, integridade e conformidade dos sistemas.

A integração com outras capabilities assegura uma resposta eficaz a incidentes.

O propósito da Event & Monitoring Management é assegurar a confiabilidade e disponibilidade dos sistemas de TI, identificando e respondendo a eventos que possam afetar a operação e desempenho dos serviços.

Esta capability é crítica para manter a eficiência operacional, fomentar a inovação e manter a vantagem competitiva da organização.

Dentro do CIO Codex Capability Framework, os objetivos da Event & Monitoring Management incluem garantir a Eficiência Operacional, facilitar a Inovação, proporcionar Vantagem Competitiva, monitorar a Infraestrutura de TI, avaliar o impacto dos eventos na Arquitetura de TI, supervisionar os Sistemas para identificar problemas de desempenho ou falhas, e integrar a supervisão contínua aos processos operacionais da organização.

O impacto desta capability nas dimensões tecnológicas é amplo.

Na Infraestrutura, assegura disponibilidade e performance dos componentes.

Na Arquitetura, avalia o impacto dos eventos e mantém a integridade arquitetônica.

Nos Sistemas, supervisiona para identificar e responder rapidamente a problemas.

Em Cybersecurity, monitora eventos de segurança para identificar ameaças.

No Modelo Operacional, integra a supervisão contínua, assegurando tratamento adequado dos eventos.

Em resumo, a Event & Monitoring Management é essencial para organizações que buscam eficiência operacional, inovação e vantagem competitiva, assegurando que os sistemas de TI sejam confiáveis, disponíveis e capazes de responder proativamente a eventos e mudanças no ambiente tecnológico.

Conceitos e Características

A Event & Monitoring Management desempenha um papel crucial na manutenção da qualidade e disponibilidade dos serviços de TI.

Sua abordagem proativa ajuda a prevenir problemas, melhorar a eficiência operacional e proporcionar uma experiência contínua e confiável para os usuários finais.

Conceitos

- Supervisão Contínua: Envolve a observação constante dos sistemas de TI, coletando dados e informações relevantes para análise.
- Eventos de TI: Refere-se a qualquer acontecimento ou mudança nos sistemas que possa indicar um problema, potencial ou real, ou impactar o desempenho.
- Monitoramento Proativo: Significa a identificação e mitigação de problemas antes que afetem os serviços, minimizando interrupções.

Características

- Alertas e Notificações: A Event & Monitoring Management emite alertas automáticos quando eventos críticos ou anomalias são detectados, permitindo uma ação rápida.
- Análise de Tendências: Além de lidar com eventos imediatos, essa capability analisa tendências a longo prazo para identificar possíveis riscos e melhorias.
- Resposta a Eventos: Define procedimentos claros para responder a eventos, restaurar a normalidade e minimizar o impacto nos serviços.

- Monitoramento Multifacetado: Supervisiona não apenas o desempenho, mas também a segurança, integridade e conformidade dos sistemas.
- Integração com outras capabilities: Trabalha em conjunto com outras capabilities, como Incident Management, para garantir uma resposta eficaz a incidentes.

Propósito e Objetivos

A capability de Event & Monitoring Management desempenha um papel fundamental na supervisão contínua dos sistemas de TI, identificando e respondendo a eventos que possam afetar a operação e desempenho dos serviços.

Seu propósito é assegurar a confiabilidade e disponibilidade dos sistemas, incluindo o monitoramento proativo para detectar e prevenir incidentes antes que eles ocorram.

Essa capability desempenha um papel crítico na manutenção da eficiência operacional, inovação e vantagem competitiva da organização.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, a Event & Monitoring Management busca atingir os seguintes objetivos:

- Eficiência Operacional: Garantir a operação contínua e eficaz dos sistemas de TI, minimizando interrupções e downtime.
- Inovação: Capacitar a organização a adotar novas tecnologias e práticas, alinhando-se às tendências de mercado.
- Vantagem Competitiva: Permitir que a organização responda rapidamente a eventos e incidentes, mantendo a continuidade dos serviços.
- Infraestrutura: Monitorar a infraestrutura de TI para garantir que recursos como servidores, redes e armazenamento estejam disponíveis e funcionando adequadamente.
- Arquitetura: Avaliar o impacto de eventos nos componentes de arquitetura e tomar medidas para manter a integridade da arquitetura.
- Sistemas: Supervisionar os sistemas de TI para identificar problemas de desempenho ou falhas e responder prontamente.

- Modelo Operacional: Integrar a supervisão contínua aos processos operacionais, garantindo que eventos sejam tratados de acordo com as políticas e procedimentos estabelecidos.

Impacto na Tecnologia

A capability de Event & Monitoring Management afeta várias dimensões tecnológicas:

- Infraestrutura: Garante a disponibilidade e o desempenho dos componentes de infraestrutura, contribuindo para a estabilidade dos serviços.
- Arquitetura: Avalia o impacto de eventos na arquitetura de TI e toma medidas para preservar a integridade arquitetônica.
- Sistemas: Supervisiona sistemas e aplicativos para identificar problemas de desempenho ou falhas, possibilitando ação imediata.
- Cybersecurity: Monitora eventos de segurança, identificando possíveis ameaças e respondendo a elas para proteger a infraestrutura de TI.
- Modelo Operacional: Integra a supervisão contínua aos processos operacionais, garantindo que os eventos sejam tratados de acordo com as políticas da organização.

Roadmap de Implementação

A capability de Event & Monitoring Management desempenha um papel crucial na manutenção da qualidade e disponibilidade dos serviços de TI.

Abaixo, um roadmap de implementação para a Event & Monitoring Management, considerando os principais pontos do CIO Codex Capability Framework:

- Definição de Objetivos Estratégicos: Inicie definindo objetivos estratégicos relacionados ao gerenciamento de eventos e monitoramento. Estabeleça metas claras, como redução de incidentes críticos e melhoria na disponibilidade de serviços.
- Identificação de Fontes de Dados: Identifique as fontes de dados relevantes, como logs de sistemas, métricas de desempenho e eventos de

segurança. Isso é fundamental para uma supervisão eficaz.

- Seleção de Ferramentas e Plataformas: Escolha as ferramentas e plataformas adequadas para coletar, processar e analisar os dados de eventos e monitoramento. Certifique-se de que elas atendam aos requisitos da organização.
- Definição de Alertas e Notificações: Configure alertas e notificações automáticas para eventos críticos ou anomalias. Isso permitirá uma resposta rápida a problemas potenciais.
- Desenvolvimento de Políticas de Resposta: Estabeleça políticas claras para a resposta a eventos. Defina procedimentos de ação, responsabilidades das equipes e escalonamento quando necessário.
- Implementação de Monitoramento Proativo: Configure sistemas de monitoramento proativo para identificar problemas antes que afetem os serviços. Isso inclui a definição de métricas de desempenho e alarmes.
- Treinamento da Equipe: Capacite a equipe responsável pelo Event & Monitoring Management, fornecendo treinamento sobre o uso das ferramentas, interpretação de dados e procedimentos de resposta.
- Integração com outras capabilities: Trabalhe em conjunto com outras capabilities, como Incident Management e Change Management, para garantir uma resposta eficaz a incidentes e mudanças relacionadas.
- Análise de Tendências: Além do monitoramento em tempo real, implemente análises de tendências a longo prazo para identificar possíveis riscos e oportunidades de melhoria.
- Testes e Validação: Realize testes de validação para garantir que os alertas e notificações estejam funcionando conforme o esperado. Isso inclui cenários de simulação de incidentes.
- Documentação Abrangente: Mantenha registros detalhados de todos os eventos monitorados, ações tomadas e lições aprendidas. Isso contribuirá para a melhoria contínua.
- Avaliação e Melhoria Contínua: Avalie regularmente o desempenho da Event & Monitoring Management e faça ajustes conforme necessário para otimizar a eficácia do processo.
- Relatórios e Comunicação: Desenvolva relatórios periódicos para comunicar o desempenho da supervisão de eventos e monitoramento às partes interessadas.

Ao seguir este roadmap, as organizações podem implementar com sucesso a capability

de Event & Monitoring Management, assegurando a confiabilidade e disponibilidade dos sistemas de TI.

Essa abordagem proativa ajuda a prevenir problemas, melhorar a eficiência operacional e proporcionar uma experiência contínua e confiável para os usuários finais, contribuindo para a qualidade e sucesso dos serviços de TI.

Melhores Práticas de Mercado

A Event & Monitoring Management desempenha um papel crítico na eficiência operacional e na garantia de uma experiência confiável para os usuários finais, adotando essas estratégias e abordagens.

Melhores Práticas de Mercado para Event & Monitoring Management:

- Supervisão Contínua: A prática de supervisão constante de sistemas de TI, coletando dados em tempo real para análise e tomada de decisões proativas.
- Alertas Automáticos: Utilização de sistemas de alerta automáticos que notificam as equipes de operação de TI quando eventos críticos ou anomalias são detectados.
- Análise Preditiva: Implementação de ferramentas de análise preditiva para identificar possíveis problemas com base em padrões históricos, permitindo ação antecipada.
- Monitoramento Multifacetado: Supervisão não apenas do desempenho, mas também da segurança, integridade e conformidade dos sistemas de TI.
- Integração com outras capabilities: Trabalho conjunto com outras capabilities, como Incident Management e Change Management, para garantir uma resposta eficaz a incidentes.
- Centralização de Logs: Armazenamento e análise centralizados de logs de eventos para identificar correlações e tendências em toda a infraestrutura de TI.
- Automatização de Resposta: Automação de procedimentos de resposta a eventos, permitindo ações rápidas e consistentes.
- Machine Learning e IA: Utilização de algoritmos de Machine Learning e

Inteligência Artificial para identificar padrões complexos e ameaças emergentes.
- Monitoramento de Nuvem: Extensão do monitoramento para ambientes de nuvem, garantindo visibilidade completa das operações de TI.
- Auditoria e Conformidade: Implementação de auditorias regulares para garantir que as práticas de Event & Monitoring estejam em conformidade com regulamentos e padrões do setor.

Essas melhores práticas são amplamente reconhecidas no mercado de TI e são essenciais para manter a qualidade, disponibilidade e segurança dos serviços de TI.

Desafios Atuais

A capability de Event & Monitoring Management, que faz parte da macro capability Service Reliability e está inserida na camada Service Excellence, desempenha um papel fundamental na manutenção da qualidade e disponibilidade dos serviços de TI.

No entanto, ao adotar e integrar essa capability em seus processos de negócios e operações de TI, as organizações enfrentam diversos desafios atuais, de acordo com as melhores práticas do mercado:

- Explosão de Dados: A quantidade de dados gerados pelos sistemas de TI está em constante crescimento, tornando desafiador o processo de monitoramento e análise em busca de eventos significativos.
- Complexidade da Infraestrutura: A crescente complexidade da infraestrutura de TI, com a adoção de tecnologias como nuvem, contêineres e microsserviços, requer uma abordagem mais sofisticada para o monitoramento.
- Diversidade Tecnológica: A coexistência de diferentes tecnologias e sistemas torna difícil a padronização do monitoramento, exigindo soluções flexíveis e integradas.
- Detecção de Ameaças Cibernéticas: A Event & Monitoring Management deve lidar com a detecção de ameaças cibernéticas em tempo real, exigindo algoritmos avançados e automação.
- Integração de Dados: Integrar dados de diversas fontes, como logs de aplicativos, dispositivos de rede e sensores de IoT, para obter uma visão

completa, é um desafio complexo.

- Identificação de Eventos Relevantes: É crucial filtrar os eventos significativos entre o grande volume de dados gerados, garantindo que a equipe possa se concentrar no que realmente importa.
- Mobilidade e Ambientes Distribuídos: A necessidade de monitorar ambientes distribuídos e dispositivos móveis exige uma abordagem que vá além dos sistemas tradicionais de data center.
- Lidar com Falsos Positivos: Evitar alertas falsos é uma preocupação, pois alertas desnecessários podem sobrecarregar as equipes de operações.
- Cultura de Proatividade: Cultivar uma cultura organizacional que valorize a proatividade na identificação e mitigação de eventos é um desafio de mudança cultural.
- Integração com Outras Capabilities: A integração eficaz com outras capabilities, como Incident Management e Problem Management, é fundamental para garantir ações coerentes em resposta a eventos.

Esses desafios ilustram a necessidade de uma abordagem abrangente e avançada para a Event & Monitoring Management no ambiente de TI atual.

Para manter a qualidade e a confiabilidade dos serviços de TI, é crucial enfrentar esses obstáculos com soluções tecnológicas e processos eficazes.

A abordagem proativa dessa capability desempenha um papel vital na prevenção de problemas, melhoria da eficiência operacional e garantia de uma experiência contínua e confiável para os usuários finais.

Tendências para o Futuro

A capability de Event & Monitoring Management, inserida na macro capability de Service Reliability e na camada Service Excellence, desempenha um papel crucial na manutenção da qualidade e disponibilidade dos serviços de TI.

Sua abordagem proativa ajuda a prevenir problemas, melhorar a eficiência operacional e proporcionar uma experiência contínua e confiável para os usuários finais.

Considerando as expectativas do mercado e as grandes tendências que podem moldar o desenvolvimento futuro da Event & Monitoring Management, as seguintes tendências:

- Inteligência Artificial e Aprendizado de Máquina: A utilização de algoritmos de IA e aprendizado de máquina se tornará mais ampla na detecção de eventos e na previsão de problemas, permitindo uma resposta ainda mais eficaz.
- Monitoramento de Experiência do Usuário (UX): A capacidade de monitorar a experiência do usuário final se tornará uma prioridade, permitindo identificar problemas de usabilidade que afetam a satisfação do cliente.
- Monitoramento de Segurança Avançado: O monitoramento de eventos de segurança será aprimorado para detectar ameaças cibernéticas em tempo real e tomar medidas imediatas para mitigar riscos.
- Automatização de Respostas: A automatização das respostas a eventos comuns se tornará mais sofisticada, permitindo que a capability lide automaticamente com problemas conhecidos.
- Monitoramento em Tempo Real em Nuvem: Com a crescente adoção de soluções em nuvem, o monitoramento em tempo real de ambientes em nuvem se tornará essencial para garantir o desempenho e a segurança.
- IoT e Edge Computing: A integração de dispositivos IoT e o crescimento da computação de borda exigirão um monitoramento mais abrangente e em tempo real para garantir a integridade desses sistemas.
- Análise de Big Data para Previsão: A análise de big data será usada para prever eventos e problemas com base em padrões históricos, permitindo uma intervenção proativa.
- Integração com DevOps: A colaboração estreita entre Event & Monitoring Management e equipes de DevOps será essencial para garantir que as alterações no código sejam monitoradas desde o início.
- Automação de Resiliência: A capacidade de automatizar a resiliência dos sistemas em resposta a eventos críticos garantirá a continuidade dos serviços.
- Monitoramento de Conformidade: O monitoramento de conformidade regulatória se tornará mais rigoroso, com a capability acompanhando e reportando automaticamente as métricas necessárias.

Essas tendências refletem a crescente importância da Event & Monitoring Management à medida que as organizações buscam manter a confiabilidade e disponibilidade de seus serviços de TI em um ambiente cada vez mais complexo e dinâmico.

A evolução dessas práticas contribuirá para a eficiência operacional, a inovação e a vantagem competitiva das organizações, além de garantir uma experiência contínua e confiável para os usuários finais.

KPIs Usuais

A capability de Event & Monitoring Management desempenha um papel crucial na manutenção da qualidade e disponibilidade dos serviços de TI.

Sua abordagem proativa ajuda a prevenir problemas, melhorar a eficiência operacional e proporcionar uma experiência contínua e confiável para os usuários finais.

Para avaliar e medir o desempenho dessa capability, é fundamental considerar os Indicadores-Chave de Desempenho (KPIs) usuais no mercado.

No contexto do CIO Codex Capability Framework, uma lista dos principais KPIs para Event & Monitoring Management:

- Tempo Médio de Detecção (Average Detection Time): Mede o tempo médio necessário para identificar eventos ou anomalias nos sistemas de TI desde o momento em que ocorrem.
- Tempo Médio de Resposta (Average Response Time): Calcula o tempo médio necessário para iniciar uma resposta ou ação após a detecção de um evento ou problema.
- Eficiência na Resolução (Resolution Efficiency): Avalia a rapidez e eficácia na resolução de eventos, minimizando o impacto nos serviços.
- Taxa de Falsos Positivos (False Positive Rate): Mede a proporção de eventos ou alertas que foram considerados problemas, mas não representaram ameaças reais.
- Disponibilidade do Monitoramento (Monitoring Availability): Avalia o tempo em que os sistemas de monitoramento estão operacionais e prontos para detectar eventos.
- Taxa de Correlação de Eventos (Event Correlation Rate): Mede a capacidade de identificar relações entre eventos e criar alertas ou ações com base nessa correlação.
- Escopo de Monitoramento (Monitoring Scope): Avalia a extensão do monitoramento, incluindo sistemas, aplicativos, servidores e redes

cobertos pela Event & Monitoring Management.

- Acurácia na Identificação de Tendências (Trend Identification Accuracy): Mede a precisão na identificação de tendências de longo prazo que podem indicar riscos ou oportunidades.
- Tempo Médio de Recuperação (Average Recovery Time): Calcula o tempo médio necessário para restaurar a normalidade após a ocorrência de um evento ou incidente.
- Taxa de Alertas Não Resolvidos (Unresolved Alert Rate): Mede a proporção de alertas ou eventos que não foram resolvidos ou fechados adequadamente.
- Impacto nos Negócios (Business Impact): Avalia o impacto dos eventos ou incidentes nos objetivos e operações do negócio, incluindo perdas financeiras e de reputação.
- Integração com outras capabilities (Integration with other capabilities): Mede a capacidade de Event & Monitoring Management em trabalhar em conjunto com outras capabilities, como Incident Management, para uma resposta eficaz a incidentes.
- Quantidade de Eventos por Período (Number of Events per Period): Contabiliza o número total de eventos ou alertas gerados e tratados durante um período específico.
- Evolução da Infraestrutura (Infrastructure Evolution): Avalia o impacto das ações de monitoramento na evolução e melhoria da infraestrutura de TI.
- Conformidade Regulatória (Regulatory Compliance): Mede a conformidade com regulamentações e normas relevantes por meio da monitorização de eventos relacionados à segurança e conformidade.

Esses KPIs são essenciais para garantir a confiabilidade, disponibilidade e eficácia das operações de TI, permitindo a detecção precoce de problemas, a rápida resposta a eventos críticos e a minimização de impactos nos serviços.

A medição adequada desses indicadores contribui para a manutenção da eficiência operacional, inovação e vantagem competitiva da organização.

Exemplos de OKRs

A capability de Event & Monitoring Management, no âmbito do CIO Codex Capability Framework, desempenha um papel essencial na monitorização e gestão de eventos e alertas de sistemas de TI.

Esta capability é crucial para garantir a detecção precoce de problemas, a resposta eficaz a eventos críticos e a manutenção da estabilidade e desempenho dos sistemas.

A seguir, são apresentados exemplos de Objetivos e Resultados-Chave (OKRs) relacionados a esta capability:

Detecção e Resposta Rápida a Eventos Críticos

Objetivo: Garantir a detecção precoce e a resposta eficaz a eventos críticos que possam afetar a operação de sistemas de TI.

- KR1: Reduzir o tempo médio de detecção de eventos críticos em 30%.
- KR2: Garantir que 100% dos eventos críticos sejam investigados e tratados dentro do prazo acordado.
- KR3: Aumentar a satisfação dos usuários em relação à resolução de incidentes em 15%.

Monitorização Proativa de Desempenho

Objetivo: Implementar uma monitorização proativa para garantir o desempenho ideal dos sistemas de TI.

- KR1: Cobrir 100% dos sistemas de TI com monitorização proativa.
- KR2: Identificar e resolver proativamente 90% dos problemas de desempenho antes que afetem os usuários.
- KR3: Melhorar a eficiência operacional em 20% por meio da monitorização proativa.

Gestão de Alertas Eficiente

Objetivo: Implementar uma gestão eficiente de alertas para priorizar e tratar alertas de maneira adequada.

- KR1: Reduzir em 50% o número de alertas falsos.
- KR2: Garantir que 100% dos alertas sejam classificados e tratados de acordo com sua prioridade.
- KR3: Melhorar a resposta a alertas críticos em 25%.

Análise de Tendências e Prevenção de Problemas Recorrentes

Objetivo: Realizar análises de tendências para identificar problemas recorrentes e implementar medidas preventivas.

- KR1: Identificar 80% dos problemas recorrentes por meio de análises de tendências.
- KR2: Reduzir em 40% a ocorrência de problemas recorrentes por meio de medidas preventivas.
- KR3: Aumentar a eficácia das análises de tendências em 15% ao longo do ano.

Alinhamento com Metas de Negócios

Objetivo: Assegurar que a monitorização e gestão de eventos estejam alinhadas com as metas de negócios da organização.

- KR1: Alinhar 90% das métricas de monitorização com os KPIs de negócios.
- KR2: Garantir que 100% dos eventos monitorizados estejam relacionados a serviços de negócios críticos.
- KR3: Realizar revisões periódicas para confirmar o alinhamento contínuo entre eventos e metas de negócios.

Esses OKRs demonstram a importância crítica da Event & Monitoring Management na detecção, resposta e prevenção de problemas nos sistemas de TI.

Através desses objetivos e resultados-chave, as organizações podem garantir a estabilidade, desempenho e disponibilidade dos sistemas de TI, contribuindo assim para o sucesso das metas de negócios e a satisfação dos usuários.

A Event & Monitoring Management desempenha um papel vital na operação eficaz de sistemas de TI e na redução de riscos operacionais.

Critérios para Avaliação de Maturidade

A capability Event & Monitoring Management desempenha um papel crucial na manutenção da confiabilidade e disponibilidade dos sistemas de TI, focando na supervisão contínua dos sistemas e na identificação e resposta a eventos que possam afetar a operação e o desempenho dos serviços.

Para avaliar a maturidade dessa capability dentro do contexto do CIO Codex Capability Framework, foram desenvolvidos critérios de avaliação inspirados no modelo CMMI, abrangendo cinco níveis de maturidade:

Nível de Maturidade Inexistente

- A organização não reconhece a necessidade de monitoramento de sistemas de TI.
- Não existem políticas ou procedimentos para supervisionar eventos.
- A supervisão de sistemas é reativa, apenas em resposta a incidentes.
- Não há ferramentas ou sistemas de monitoramento implementados.
- Não há registro ou análise de eventos passados.

Nível de Maturidade Inicial

- Reconhecimento inicial da importância do monitoramento de sistemas.
- Políticas e procedimentos iniciais estão em desenvolvimento.
- A supervisão é principalmente reativa, com algum monitoramento proativo.
- Ferramentas de monitoramento estão em fase de implementação.
- Eventos passados são registrados, mas análises são limitadas.

Nível de Maturidade Definido

- Políticas e procedimentos para monitoramento de sistemas estão estabelecidos e documentados.

- A supervisão é uma combinação equilibrada de reativa e proativa.
- Ferramentas de monitoramento estão em uso e configuradas para alertar em tempo real.
- Eventos passados são registrados e analisados para melhorias.
- Métricas de desempenho de supervisão são coletadas e monitoradas.

Nível de Maturidade Gerenciado

- O monitoramento de sistemas é regularmente monitorado e medido.
- Métricas são usadas para aprimorar as estratégias de supervisão.
- Supervisão proativa é a norma, com intervenções preventivas.
- Ferramentas de monitoramento são altamente eficazes e controladas.
- Análises avançadas são realizadas para prever eventos e otimizar a supervisão.

Nível de Maturidade Otimizado

- A supervisão de sistemas é altamente automatizada e eficaz.
- Processos são altamente otimizados e eficientes.
- Monitoramento proativo e preventivo é altamente eficiente.
- Ferramentas de monitoramento são altamente adaptáveis às necessidades em constante evolução.
- Análises avançadas de dados são usadas para aprimorar continuamente a supervisão.

Esses critérios de maturidade são essenciais para garantir que a capability Event & Monitoring Management seja capaz de supervisionar sistemas de TI de forma eficaz, identificar eventos críticos e responder proativamente, garantindo a confiabilidade e disponibilidade dos serviços de TI.

À medida que a organização avança nos níveis de maturidade, ela se torna mais capaz de prevenir incidentes e manter a integridade dos sistemas de TI, atendendo às expectativas dos stakeholders e mantendo a excelência em serviços de TI.

Convergência com Frameworks de Mercado

A capability Event & Monitoring Management, pertencente à macro capability Service Reliability e localizada na camada Service Excellence, é fundamental na supervisão contínua dos sistemas de TI.

Esta capability especializa-se na identificação e resposta a eventos que podem impactar a operação e o desempenho dos serviços, incluindo monitoramento proativo para detectar e prevenir incidentes, garantindo a confiabilidade e disponibilidade dos sistemas.

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: COBIT oferece diretrizes detalhadas para governança de TI, incluindo a gestão de eventos e monitoramento, assegurando alinhamento com os objetivos de negócio e compliance.

ITIL

- Nível de Convergência: Alto
- Racional: ITIL possui uma estrutura robusta para o gerenciamento de serviços de TI, abrangendo práticas específicas para Event & Monitoring Management, essenciais para o gerenciamento eficaz de serviços.

SAFe

- Nível de Convergência: Médio
- Racional: SAFe foca em agilidade e escalabilidade em grandes organizações, mas reconhece a importância do monitoramento contínuo como parte da entrega contínua e integração de TI.

PMI

- Nível de Convergência: Médio
- Racional: O PMI fornece um framework para gerenciamento de projetos que pode ser aplicado na coordenação e monitoramento de eventos de TI, embora não seja especificamente focado nesta área.

CMMI

- Nível de Convergência: Médio
- Racional: CMMI aborda a melhoria de processos, que é relevante para Event & Monitoring Management, mas não fornece diretrizes específicas para esta área.

TOGAF

- Nível de Convergência: Baixo
- Racional: TOGAF, focado em arquitetura empresarial, tem um alinhamento indireto com Event & Monitoring Management, concentrando-se mais na estruturação de sistemas.

DevOps SRE

- Nível de Convergência: Alto
- Racional: DevOps SRE enfatiza a eficiência operacional e automação, alinhando-se diretamente com os objetivos de Event & Monitoring Management em termos de detecção proativa e resposta rápida a eventos.

NIST

- Nível de Convergência: Médio
- Racional: NIST, com foco em padrões de segurança, oferece diretrizes relevantes para a monitorização de eventos, especialmente em termos de

segurança e resposta a incidentes.

Six Sigma

- Nível de Convergência: Baixo
- Racional: Six Sigma, que visa à melhoria de processos e redução de defeitos, pode influenciar indiretamente as práticas de Event & Monitoring Management, mas não é especificamente focado nesta área.

Lean IT

- Nível de Convergência: Baixo
- Racional: Lean IT, com seu enfoque em eficiência e eliminação de desperdícios, pode contribuir indiretamente para otimizar processos de monitoramento de eventos.

Em síntese, Event & Monitoring Management apresenta alta convergência com frameworks focados em governança e gestão de TI como COBIT e ITIL, e também com práticas operacionais eficientes como DevOps SRE.

Frameworks focados em gerenciamento de projetos e melhoria de processos, como PMI e CMMI, mostram convergência moderada. NIST, Six Sigma e Lean IT têm uma relação mais indireta com esta capability.

Processos e Atividades

Develop Event Monitoring Plans

Desenvolver planos de monitoramento de eventos é um processo essencial para garantir a supervisão contínua e eficaz dos sistemas de TI.

Este processo envolve a criação de planos detalhados que definem os parâmetros de monitoramento, as tecnologias e ferramentas a serem utilizadas, e os procedimentos a serem seguidos para a coleta, análise e resposta a eventos.

O desenvolvimento dos planos inclui a identificação de pontos críticos de monitoramento, a definição de métricas de desempenho e a elaboração de estratégias para a mitigação de riscos potenciais.

O planejamento detalhado é crucial para garantir que todas as áreas relevantes sejam cobertas e que o monitoramento seja realizado de maneira consistente e eficiente.

Além disso, é fundamental incluir procedimentos para a revisão e atualização contínua dos planos, assegurando que eles se mantenham alinhados com as necessidades e prioridades da organização.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Define Monitoring Objectives	Definir os objetivos específicos do monitoramento de eventos.	Estratégia de TI, metas de negócios	Objetivos de monitoramento definidos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Architecture & Technology Visioning; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
2	Identify Critical Points	Identificar os pontos críticos de monitoramento nos sistemas de TI.	Objetivos de monitoramento, documentação técnica	Pontos críticos identificados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation

3	Select Monitoring Tools	Selecionar as ferramentas e tecnologias apropriadas para o monitoramento.	Pontos críticos identificados, requisitos técnicos	Ferramentas de monitoramento selecionadas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Architecture & Technology Visioning	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Architecture & Technology Visioning; Executer: IT Infrastructure & Operation
4	Develop Monitoring Procedures	Desenvolver procedimentos detalhados para a coleta, análise e resposta a eventos.	Ferramentas selecionadas, melhores práticas	Procedimentos de monitoramento desenvolvidos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
5	Document Monitoring Plan	Documentar o plano de monitoramento de eventos, incluindo objetivos, pontos críticos e procedimentos.	Procedimentos desenvolvidos, objetivos de monitoramento	Plano de monitoramento documentado	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: IT Governance & Transformation; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation

Identify Monitoring Requirements

Identificar os requisitos de monitoramento é um processo crucial que visa garantir que todas as necessidades e condições para uma supervisão eficaz dos sistemas de TI sejam claramente definidas e documentadas.

Este processo envolve a coleta e análise de informações detalhadas sobre os componentes a serem monitorados, incluindo requisitos técnicos, funcionais e de

segurança.

Além disso, é fundamental considerar as dependências com outros sistemas e serviços, bem como os impactos potenciais nas operações do negócio.

A validação dos requisitos com as partes interessadas é uma etapa crítica para garantir que todas as expectativas sejam atendidas e que os objetivos de monitoramento sejam alcançados de forma eficaz.

A documentação dos requisitos serve como base para o planejamento e execução das atividades de monitoramento, proporcionando clareza e direcionamento para todas as equipes envolvidas.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Collect Requirement Data	Coletar dados detalhados sobre os requisitos de monitoramento.	Propostas de mudança, feedback dos usuários	Dados coletados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
2	Analyze Technical Needs	Analisar as necessidades técnicas para o monitoramento, incluindo hardware e software.	Dados coletados, documentação técnica	Relatório de análise técnica	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Architecture & Technology Visioning; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation

3	Identify Functional Requirements	Identificar os requisitos funcionais do monitoramento.	Relatório de análise técnica, dados de requisitos funcionais	Lista de requisitos funcionais	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
4	Validate Requirements	Validar os requisitos identificados com as partes interessadas.	Lista de requisitos funcionais, feedback dos stakeholders	Requisitos validados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: IT Governance & Transformation; Informed: Architecture & Technology Visioning	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: IT Infrastructure & Operation
5	Document Monitoring Requirements	Documentar todos os requisitos de monitoramento de forma clara e compreensível.	Requisitos validados, melhores práticas	Documentação de requisitos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation

Implement Monitoring Solutions

Implementar soluções de monitoramento conforme planejado é um processo vital para garantir que as ferramentas e procedimentos de supervisão sejam configurados e operem de maneira eficaz.

Este processo envolve a instalação e configuração de tecnologias de monitoramento, a integração dessas tecnologias com os sistemas existentes e a realização de testes para assegurar que funcionem conforme o esperado.

Durante a implementação, é crucial monitorar o progresso e resolver quaisquer problemas que possam surgir, garantindo que todas as etapas sejam concluídas conforme o cronograma estabelecido. A comunicação constante com as partes interessadas é fundamental para assegurar que todos estejam informados sobre o status da implementação e que possam fornecer feedback em tempo real.

A documentação das atividades de implementação é essencial para garantir a rastreabilidade e a transparência ao longo de todo o processo.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Install Monitoring Tools	Instalar as ferramentas de monitoramento selecionadas.	Ferramentas selecionadas, infraestrutura de TI	Ferramentas instaladas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation

2	Configure Monitoring Tools	Configurar as ferramentas de monitoramento conforme as especificações.	Ferramentas instaladas, requisitos de monitoramento	Ferramentas configuradas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Architecture & Technology Visioning; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
3	Integrate Monitoring Solutions	Integrar as soluções de monitoramento com os sistemas existentes.	Ferramentas configuradas, sistemas existentes	Soluções integradas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
4	Test Monitoring Solutions	Realizar testes para garantir que as soluções de monitoramento funcionem conforme o esperado.	Soluções integradas, plano de testes	Relatório de testes	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation

5	Communicate Implementation Status	Comunicar o status da implementação às partes interessadas.	Relatório de testes, feedback dos stakeholders	Comunicação de status	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: Architecture & Technology Visioning	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: IT Infrastructure & Operation

Monitor Event Performance

Monitorar continuamente o desempenho dos eventos é fundamental para garantir que os sistemas de TI funcionem de acordo com os padrões estabelecidos e que quaisquer anomalias sejam rapidamente identificadas e tratadas.

Este processo envolve a coleta e análise de dados em tempo real, a identificação de padrões e tendências, e a geração de alertas automáticos quando eventos críticos ou anomalias são detectados.

A comunicação constante com as partes interessadas e a documentação detalhada das atividades de monitoramento são cruciais para assegurar a transparência e a eficácia do processo.

Além disso, o monitoramento contínuo permite uma resposta proativa a problemas potenciais, minimizando interrupções nos serviços e garantindo a continuidade das operações.

A utilização de tecnologias avançadas de monitoramento e a integração com outras capacidades, como Incident Management, são essenciais para o sucesso deste processo.

- PDCA focus: Check
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Collect Real-Time Data	Coletar dados em tempo real dos sistemas de TI.	Sistemas de TI, ferramentas de monitoramento	Dados coletados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
2	Analyze Data	Analisar os dados coletados para identificar padrões e tendências.	Dados coletados, ferramentas analíticas	Relatório de análise	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Architecture & Technology Visioning; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation
3	Generate Alerts	Gerar alertas automáticos para eventos críticos e anomalias detectadas.	Relatório de análise, ferramentas de monitoramento	Alertas gerados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation

4	Respond to Alerts	Responder prontamente aos alertas gerados, tomando as ações necessárias.	Alertas gerados, procedimentos de resposta	Problemas resolvidos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: Architecture & Technology Visioning	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: IT Infrastructure & Operation
5	Document Monitoring Activities	Documentar todas as atividades de monitoramento e resposta.	Problemas resolvidos, feedback dos usuários	Documentação de atividades	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation

Review and Optimize Monitoring Processes

Revisar e otimizar os processos de monitoramento com base nos resultados obtidos é uma etapa crucial para assegurar a melhoria contínua e a eficácia das atividades de supervisão.

Este processo envolve a análise detalhada dos dados de desempenho e feedbacks coletados, a identificação de áreas de melhoria e a implementação de mudanças nos processos de monitoramento.

A revisão deve considerar as lições aprendidas, as melhores práticas do setor e as tendências de desempenho, garantindo que as estratégias de monitoramento permaneçam alinhadas com os objetivos organizacionais e as necessidades operacionais.

A documentação das mudanças e a comunicação eficaz com todas as partes

interessadas são essenciais para garantir que as melhorias sejam compreendidas e implementadas de maneira eficiente.

Este processo assegura que as atividades de monitoramento continuem a proporcionar valor significativo à organização, permitindo uma resposta proativa e eficaz a eventos e incidentes.

- PDCA focus: Act
- Periodicidade: Trimestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Evaluate Monitoring Results	Avaliar os resultados das atividades de monitoramento.	Dados de desempenho, feedback dos stakeholders	Relatório de avaliação	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
2	Identify Improvement Areas	Identificar áreas de melhoria com base na avaliação dos resultados.	Relatório de avaliação, feedback dos stakeholders	Lista de áreas de melhoria	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Architecture & Technology Visioning; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation

3	Update Monitoring Processes	Atualizar os processos de monitoramento para incorporar as melhorias identificadas.	Lista de áreas de melhoria, melhores práticas	Processos de monitoramento atualizados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
4	Document Changes	Documentar as mudanças nos processos de monitoramento.	Processos de monitoramento atualizados, feedback dos stakeholders	Documentação de mudanças	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
5	Communicate Updates	Comunicar as atualizações dos processos aos stakeholders relevantes.	Documentação de mudanças, plano de comunicação	Comunicação de atualizações	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Architecture & Technology Visioning; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation