A IT Regulatory, Audit & Compliance Management, uma capability crucial dentro da macro capability IT Governance e integrante da camada IT Transformation do CIO Codex Capability Framework, é fundamental para a governança eficaz de TI.

Esta capability assegura que a organização opere de maneira ética, legal e segura, aderindo à normas e regulamentos relevantes.

Ela tem um papel preponderante na identificação, avaliação e gerenciamento dos riscos de conformidade, ajudando a mitigar ameaças potenciais e a manter a integridade das operações de TI.

Este pilar é vital para fortalecer a confiança das partes interessadas e a reputação da

organização no seu conjunto.

Os conceitos-chave incluem Conformidade Regulatória, que se refere à aderência às leis, regulamentos governamentais e padrões do setor, Gestão de Auditorias, que abrange a organização e a avaliação de auditorias internas e externas, Identificação de Riscos de Conformidade, Controles de Conformidade, e Normas Setoriais, que são diretrizes específicas que a TI deve seguir, frequentemente relacionadas à segurança da informação e privacidade de dados.

As características desta capability incluem Mapeamento Regulatório, realização de Auditorias Internas e Externas, Gestão de Riscos, Documentação e Relatórios, e Treinamento em Conformidade.

Estas características são essenciais para assegurar que a TI opere dentro dos parâmetros legais e regulatórios, mantendo registros detalhados e proporcionando treinamento adequado à equipe.

O propósito central da IT Regulatory, Audit & Compliance Management é assegurar a conformidade legal e regulatória da TI, mitigando riscos e protegendo a organização de potenciais penalidades e danos à reputação.

Ela tem como objetivos garantir a Conformidade Legal, gerenciar Auditorias, identificar Riscos de Conformidade, implementar Controles e relatar a Conformidade para as partes interessadas.

O impacto desta capability na tecnologia é significativo, influenciando diversas dimensões como Infraestrutura, Arquitetura, Sistemas, Modelo Operacional e Cybersecurity.

Na Infraestrutura, a conformidade regulatória pode afetar as decisões relacionadas à escolha de soluções e serviços. Na Arquitetura, pode ser necessário implementar estruturas de segurança específicas.

Nos Sistemas, os sistemas de TI devem estar configurados e monitorados para cumprir os requisitos regulatórios.

No Modelo Operacional, a gestão de conformidade afeta as políticas e procedimentos operacionais.

Em Cybersecurity, a conformidade regulatória é essencial para evitar penalidades e manter os ativos protegidos.

Em resumo, a IT Regulatory, Audit & Compliance Management é uma capability essencial que permeia todas as atividades da TI, garantindo que as operações sejam conduzidas de forma ética e em total conformidade com as normas legais e

regulatórias.

Ela não apenas protege a organização de riscos legais e regulatórios, mas também contribui para a manutenção de uma imagem corporativa positiva e a confiança das partes interessadas.

A sua implementação e manutenção eficazes são, portanto, fundamentais para a sustentabilidade e o sucesso a longo prazo da organização.

Conceitos e Características

A IT Regulatory, Audit & Compliance Management é um pilar essencial da governança de TI, garantindo que a organização opere de maneira ética, legal e segura.

Sua abordagem metódica para identificar, avaliar e gerenciar riscos de conformidade ajuda a mitigar potenciais ameaças e a manter a integridade das operações de TI, fortalecendo a confiança das partes interessadas e a reputação da organização como um todo.

Conceitos

- Conformidade Regulatória: Refere-se à aderência estrita da TI às leis, regulamentos governamentais e normas do setor que se aplicam às suas operações.
- Gestão de Auditorias: Envolve o planejamento, condução e avaliação de auditorias internas e externas para avaliar o cumprimento das políticas e procedimentos.
- Identificação de Riscos de Conformidade: Consiste em identificar e avaliar os riscos potenciais relacionados à conformidade e aos impactos negativos que podem resultar de seu não cumprimento.
- Controles de Conformidade: São medidas, políticas e procedimentos implementados para mitigar os riscos de não conformidade e garantir que a TI esteja operando dentro dos padrões estabelecidos.
- Normas Setoriais: Referem-se às diretrizes específicas do setor que a TI deve seguir, muitas vezes relacionadas à segurança da informação e privacidade de dados.

Características

- Mapeamento Regulatório: Realiza uma análise minuciosa das leis e regulamentos relevantes que se aplicam à TI e mantém um registro atualizado desses requisitos.
- Auditorias Internas e Externas: Planeja, coordena e executa auditorias para avaliar a conformidade e identificar oportunidades de melhoria.
- Gestão de Riscos: Mantém um processo contínuo de identificação e avaliação de riscos de conformidade, desenvolvendo estratégias para mitigá-los.
- Documentação e Relatórios: Mantém registros detalhados de atividades de conformidade e gera relatórios para demonstrar a conformidade perante as partes interessadas internas e externas.
- Treinamento em Conformidade: Oferece treinamento e conscientização para a equipe de TI sobre as políticas e procedimentos de conformidade.

Propósito e Objetivos

A IT Regulatory, Audit & Compliance Management desempenha um papel fundamental na governança de TI, sendo essencial para garantir que a área de Tecnologia da Informação esteja em conformidade com leis, regulamentos e normas aplicáveis.

Seu propósito central é assegurar que a TI atenda às obrigações regulatórias e cumpra os requisitos legais, mitigando riscos e protegendo a organização de potenciais penalidades e danos à reputação.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, os objetivos da IT Regulatory, Audit & Compliance Management são:

- Garantir Conformidade Legal: Assegurar que a TI esteja em total conformidade com as leis e regulamentos que impactam suas operações, como leis de proteção de dados, regulamentações de segurança cibernética e requisitos de retenção de registros.

- Gerenciar Auditorias: Planejar e executar auditorias regulares para avaliar a conformidade da TI e identificar possíveis não conformidades ou áreas de melhoria.
- Identificar Riscos de Conformidade: Realizar avaliações de risco para identificar potenciais áreas de não conformidade e implementar medidas corretivas e preventivas.
- Implementar Controles: Desenvolver e implementar controles internos e políticas que garantam a conformidade contínua e a adesão aos padrões regulatórios.
- Relatar Conformidade: Preparar relatórios de conformidade para partes interessadas internas e externas, incluindo órgãos reguladores e órgãos de supervisão.

Impacto na Tecnologia

A IT Regulatory, Audit & Compliance Management influencia significativamente diversas dimensões da tecnologia:

- Infraestrutura: A definição de requisitos regulatórios pode impactar as decisões relacionadas à infraestrutura, como a escolha de provedores de serviços em nuvem ou soluções de armazenamento de dados em conformidade com regulamentos específicos.
- Arquitetura: Pode ser necessário implementar arquiteturas de segurança específicas para garantir a conformidade com regulamentos de privacidade de dados e segurança cibernética.
- Sistemas: Sistemas de TI devem ser configurados e monitorados para cumprir os requisitos regulatórios, incluindo a proteção de dados pessoais e a manutenção de registros.
- Modelo Operacional: A gestão de conformidade envolve a definição de políticas e procedimentos que afetam o modelo operacional da TI, garantindo que as atividades estejam alinhadas com os requisitos regulatórios.
- Cybersecurity: O cumprimento de regulamentações de segurança é essencial para evitar penalidades e manter os ativos protegidos.

Roadmap de Implementação

A IT Regulatory, Audit & Compliance Management, dentro do contexto do CIO Codex Capability Framework, é uma capability crucial na governança de TI, atuando como um pilar fundamental para garantir que a organização opere em conformidade com as leis, regulamentos e normas aplicáveis.

Sua abordagem metódica visa identificar, avaliar e gerenciar riscos de conformidade, reduzindo ameaças potenciais e preservando a integridade das operações de TI.

Neste texto, o roadmap de implementação dessa capability, destacando as principais etapas a serem consideradas.

- Avaliação Inicial de Conformidade: Inicie o processo de implementação com uma avaliação detalhada das regulamentações, leis e normas aplicáveis à TI. Isso inclui leis de proteção de dados, regulamentações de segurança cibernética e qualquer requisito específico do setor. Identifique as áreas de não conformidade existentes e potenciais riscos.
- Definição de Objetivos e Metas: Estabeleça objetivos claros para a conformidade, alinhados com os requisitos regulatórios e os objetivos estratégicos da organização. Defina indicadores-chave de desempenho (KPIs) para medir o progresso em relação aos objetivos de conformidade.
- Mapeamento Regulatório: Realize uma análise minuciosa das leis, regulamentos e normas identificados na etapa de avaliação inicial. Mantenha um registro atualizado desses requisitos regulatórios, incluindo datas de vencimento e responsáveis pela conformidade.
- Implementação de Controles de Conformidade: Desenvolva e implemente controles internos, políticas e procedimentos que garantam a conformidade contínua com os requisitos regulatórios. Certifique-se de que os controles sejam adequados e eficazes.
- Treinamento em Conformidade: Ofereça treinamento e conscientização para a equipe de TI sobre as políticas e procedimentos de conformidade. Certifique-se de que todos os membros da equipe compreendam suas responsabilidades em relação à conformidade.
- Gestão de Auditorias: Planeje e execute auditorias regulares para avaliar a conformidade da TI com os requisitos regulatórios. Isso inclui auditorias internas e externas, bem como a coordenação com auditores externos, se aplicável.

- Identificação e Mitigação de Riscos: Mantenha um processo contínuo de identificação e avaliação de riscos de conformidade. Desenvolva estratégias para mitigar os riscos identificados e implemente medidas corretivas quando necessário.
- Documentação e Relatórios de Conformidade: Mantenha registros detalhados de atividades de conformidade, auditorias e resultados de avaliações de risco. Prepare relatórios de conformidade para partes interessadas internas e externas, demonstrando a aderência aos requisitos regulatórios.
- Monitoramento Contínuo e Melhoria: Estabeleça um processo de monitoramento contínuo da conformidade e da eficácia dos controles internos. Identifique oportunidades de melhoria e ajuste as práticas de conformidade conforme necessário.

A implementação eficaz da IT Regulatory, Audit & Compliance Management assegura que a TI opere em conformidade com os regulamentos, protegendo a organização de penalidades legais e danos à reputação.

Além disso, promove a transparência, a confiança das partes interessadas e a sustentabilidade das operações de TI.

Melhores Práticas de Mercado

No contexto do CIO Codex Capability Framework, a capability de IT Regulatory, Audit & Compliance Management desempenha um papel crítico na governança de TI, garantindo que a organização opere de forma ética, legal e segura.

As melhores práticas de mercado nesta área são fundamentais para mitigar riscos de conformidade, proteger a integridade das operações de TI e manter a confiança das partes interessadas.

A seguir, as principais melhores práticas de mercado:

- Mapeamento Regulatório Abrangente: Realizar um mapeamento minucioso das leis, regulamentos e normas aplicáveis à TI e manter um registro atualizado desses requisitos. Isso inclui leis de privacidade de dados, regulamentações de segurança cibernética e normas específicas do

setor.

- Auditorias Regulares: Planejar e conduzir auditorias internas e externas de forma regular para avaliar o cumprimento das políticas e procedimentos de conformidade. As auditorias fornecem insights valiosos e identificam áreas de melhoria.
- Gestão Proativa de Riscos de Conformidade: Estabelecer um processo contínuo de identificação e avaliação de riscos de conformidade. Isso envolve a análise de impacto de possíveis não conformidades e a implementação de medidas corretivas e preventivas.
- Implementação de Controles de Conformidade: Desenvolver e implementar controles internos, políticas e procedimentos que garantam a conformidade contínua com os requisitos regulatórios. Isso inclui a definição de responsabilidades claras.
- Documentação e Relatórios Detalhados: Manter registros detalhados das atividades de conformidade, incluindo documentação de auditorias, avaliações de risco e ações corretivas. Gerar relatórios que demonstrem a conformidade perante partes interessadas internas e externas.
- Treinamento e Conscientização: Oferecer treinamento regular para a equipe de TI sobre as políticas e procedimentos de conformidade. A conscientização é fundamental para o cumprimento das diretrizes estabelecidas.
- Acompanhamento de Alterações Regulatórias: Manter-se atualizado sobre alterações nas leis e regulamentos que possam afetar a TI. Isso inclui a adaptação ágil às mudanças nas obrigações regulatórias.
- Criação de uma Cultura de Conformidade: Desenvolver uma cultura organizacional que valorize a conformidade como um elemento central das operações de TI. Isso requer o envolvimento de todos os membros da equipe.
- Colaboração com Órgãos Reguladores: Estabelecer canais de comunicação eficazes com órgãos reguladores e agências governamentais relevantes. Isso ajuda a manter uma relação transparente e a obter orientações claras.
- Avaliação de Terceiros e Fornecedores: Avaliar regularmente terceiros e fornecedores de TI para garantir que eles também estejam em conformidade com as regulamentações aplicáveis. Isso reduz riscos de conformidade externos.
- Auditoria de Sistemas e Dados: Realizar auditorias específicas de sistemas

e dados para garantir que as práticas de segurança da informação estejam em conformidade com regulamentos de proteção de dados e privacidade.

A implementação dessas melhores práticas de mercado na capability de IT Regulatory, Audit & Compliance Management é fundamental para proteger a organização de potenciais penalidades legais, danos à reputação e riscos operacionais.

Além disso, contribui para fortalecer a confiança das partes interessadas e manter a integridade das operações de TI.

Desafios Atuais

A IT Regulatory, Audit & Compliance Management desempenha um papel crítico na governança de TI, garantindo que as operações de tecnologia da informação sejam conduzidas em conformidade com as leis, regulamentos e normas aplicáveis.

Entretanto, ao adotar e integrar essa capability em processos de negócios e operações de TI, as organizações se deparam com vários desafios atuais, baseados nas melhores práticas de mercado.

Abaixo, uma lista dos principais desafios enfrentados pelas organizações no contexto do CIO Codex Capability Framework:

- Evolução das Regulamentações: As regulamentações e leis relacionadas à TI estão em constante evolução, o que torna desafiador acompanhar e adaptar-se às mudanças de forma eficaz.
- Complexidade das Normas Setoriais: Setores específicos, como serviços financeiros e saúde, têm regulamentos altamente complexos que requerem esforços significativos para garantir a conformidade.
- Gestão de Dados em Conformidade: A proteção e o gerenciamento de dados em conformidade com regulamentos de privacidade, como o GDPR, são desafios crescentes, especialmente em organizações com grandes volumes de dados.
- Riscos Cibernéticos em Ascensão: A crescente sofisticação das ameaças cibernéticas torna a garantia da conformidade com regulamentos de segurança uma tarefa complexa.

- Avaliação de Terceiros: Avaliar a conformidade de parceiros e fornecedores terceirizados pode ser demorado e desafiador, mas é fundamental para garantir a conformidade em toda a cadeia de suprimentos.
- Custos de Conformidade: Investir em tecnologias e recursos para garantir a conformidade pode ser dispendioso, especialmente para organizações menores com recursos limitados.
- Treinamento e Conscientização: Garantir que a equipe de TI esteja ciente das políticas e regulamentos de conformidade e seja devidamente treinada é um desafio constante.
- Relatórios e Documentação: Manter registros detalhados de atividades de conformidade e gerar relatórios para demonstrar a conformidade perante partes interessadas internas e externas requer eficiência e precisão.
- Desafios Globais: Para organizações com operações globais, a conformidade com regulamentações de diferentes países pode ser complexa e envolver uma grande variedade de requisitos.
- Auditorias Externas: A preparação e o gerenciamento de auditorias externas podem ser intensivos em termos de tempo e recursos, especialmente quando realizadas por órgãos reguladores.

Enfrentar esses desafios é essencial para garantir que a IT Regulatory, Audit & Compliance Management atinja seus objetivos.

Isso requer um compromisso constante com a atualização das regulamentações, o desenvolvimento de práticas sólidas de gestão de dados, a implementação de medidas de segurança cibernética robustas e a criação de uma cultura de conformidade em toda a organização.

Além disso, as organizações devem estar dispostas a investir em recursos e tecnologias para manter a conformidade em um ambiente de negócios em constante mudança.

O sucesso nessa área não apenas protege a organização de penalidades e danos à reputação, mas também constrói confiança entre as partes interessadas e reforça a integridade das operações de TI.

Tendências para o Futuro

A IT Regulatory, Audit & Compliance Management é um elemento vital da governança de TI, garantindo que as operações de Tecnologia da Informação ocorram em conformidade com leis, regulamentos e padrões relevantes.

É essencial explorar as tendências futuras que moldarão o desenvolvimento dessa capability para atender às crescentes demandas regulatórias e de conformidade.

Abaixo, as principais tendências para o futuro dentro do contexto do CIO Codex Capability Framework:

- Automatização de Auditorias e Conformidade: A automação de processos de auditoria e conformidade utilizará IA e aprendizado de máquina para acelerar a identificação de não conformidades e melhorar a eficiência das auditorias.
- Conformidade Regulatória Global: Com as organizações operando em escala global, as regulamentações transfronteiriças se tornarão mais complexas. A capacidade de acompanhar e cumprir regulamentos em diferentes jurisdições será essencial.
- Privacidade de Dados e LGPD: O foco na privacidade de dados e o cumprimento da Lei Geral de Proteção de Dados (LGPD) no Brasil continuarão a ser tendências críticas, com regulamentos semelhantes em outros países.
- Blockchain para Auditoria e Integridade de Dados: A tecnologia blockchain será amplamente utilizada para registrar auditorias e garantir a integridade dos dados de conformidade.
- Auditorias em Tempo Real: A capacidade de realizar auditorias em tempo real, monitorando continuamente a conformidade, ganhará importância para identificar e resolver problemas rapidamente.
- Cibersegurança e Conformidade: A interseção entre cibersegurança e conformidade será mais destacada, com regulamentos exigindo medidas rigorosas de segurança de dados.
- Conformidade Digital: Com a transformação digital, as organizações precisarão garantir a conformidade em ambientes digitais, como plataformas de e-commerce e aplicativos móveis.
- Ética da IA e da Automatização: A conformidade com princípios éticos na implementação de IA e processos automatizados será uma tendência

crítica, exigindo auditorias específicas para avaliar o impacto das decisões algorítmicas.
- Conformidade com Sustentabilidade: À medida que as preocupações ambientais crescem, a conformidade com regulamentações relacionadas à sustentabilidade e responsabilidade social corporativa se tornará essencial.
- Colaboração em Conformidade: A colaboração entre equipes de conformidade, TI e jurídicas se intensificará, já que as regulamentações se tornam mais interdisciplinares.

Essas tendências refletem a crescente complexidade e importância da IT Regulatory, Audit & Compliance Management na governança de TI.

À medida que as organizações enfrentam um ambiente regulatório em constante evolução, a capacidade de antecipar e se adaptar a essas tendências será essencial para garantir a conformidade e a integridade operacional.

KPIs Usuais

A capability IT Regulatory, Audit & Compliance Management desempenha um papel crítico na governança de TI, garantindo que a organização atue de acordo com as leis, regulamentos e normas aplicáveis.

Para avaliar o sucesso e a eficácia dessa capability, é essencial monitorar KPIs relevantes que demonstrem o cumprimento das obrigações regulatórias e o gerenciamento adequado dos riscos de conformidade.

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

- Taxa de Conformidade Legal: Mede o grau de conformidade da TI com as leis e regulamentos relevantes, como leis de proteção de dados, regulamentações de segurança cibernética e requisitos de retenção de registros.
- Taxa de Sucesso em Auditorias: Avalia a eficácia da gestão de auditorias, medindo quantas auditorias resultam em conformidade com as políticas e procedimentos.

- Taxa de Identificação de Riscos de Conformidade: Monitora a capacidade da TI de identificar e avaliar riscos potenciais relacionados à conformidade e aos impactos negativos que podem resultar de seu não cumprimento.
- Taxa de Implementação de Controles de Conformidade: Calcula o progresso na implementação de controles internos e políticas para mitigar os riscos de não conformidade.
- Taxa de Relatórios de Conformidade: Avalia a eficiência na preparação e apresentação de relatórios de conformidade para partes interessadas internas e externas, incluindo órgãos reguladores.
- Taxa de Atualização do Mapeamento Regulatório: Mede a frequência com que o mapeamento das leis e regulamentos relevantes é atualizado para refletir as mudanças na legislação.
- Taxa de Conscientização sobre Políticas de Conformidade: Avalia o nível de conscientização da equipe de TI sobre as políticas e procedimentos de conformidade.
- Taxa de Resolução de Não Conformidades: Monitora a eficácia na identificação e resolução de não conformidades identificadas durante auditorias e avaliações de conformidade.
- Taxa de Adesão a Normas Setoriais: Calcula o grau de adesão às diretrizes específicas do setor relacionadas à segurança da informação e privacidade de dados.
- Taxa de Treinamento em Conformidade: Avalia o envolvimento da equipe de TI em treinamentos para desenvolver habilidades de conformidade.
- Taxa de Atualização de Documentação e Relatórios: Mede a frequência com que a documentação de conformidade e os relatórios são atualizados e mantidos.
- Taxa de Resposta a Incidentes de Conformidade: Monitora a capacidade da TI de responder a incidentes de conformidade de maneira eficaz e dentro dos prazos definidos.
- Taxa de Preparação para Auditorias Externas: Avalia o preparo da TI para auditorias externas, incluindo a documentação e os recursos necessários.
- Taxa de Avaliação de Impacto de Novas Regulamentações: Calcula a rapidez com que a TI avalia o impacto de novas regulamentações em suas operações e implementa as mudanças necessárias.
- Taxa de Alinhamento com Objetivos Estratégicos: Mede o grau de alinhamento das atividades de conformidade com os objetivos estratégicos

da organização, garantindo que a conformidade seja um ponto central na estratégia global.

Esses KPIs são cruciais para avaliar o desempenho da IT Regulatory, Audit & Compliance Management, garantindo que ela alcance seus objetivos de garantir conformidade legal, gerenciar auditorias eficazes, identificar riscos de conformidade e implementar controles adequados.

Além disso, eles ajudam a manter a integridade das operações de TI, fortalecer a confiança das partes interessadas e proteger a reputação da organização.

Exemplos de OKRs

A capability de IT Regulatory, Audit & Compliance Management desempenha um papel fundamental na garantia de que a TI esteja em conformidade com leis, regulamentos e normas.

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

Garantia de Conformidade Regulatória

Objetivo: Assegurar que a TI esteja em conformidade com todas as leis, regulamentos e normas relevantes.

- KR1: Realizar uma análise completa das regulamentações aplicáveis à TI e identificar os requisitos de conformidade.
- KR2: Desenvolver um plano de conformidade que inclua a implementação de controles específicos para atender a esses requisitos.
- KR3: Realizar auditorias internas regulares para verificar o cumprimento das obrigações regulatórias.

Identificação e Mitigação de Riscos de Conformidade

Objetivo: Identificar e mitigar proativamente os riscos de conformidade que podem afetar a TI.

- KR1: Realizar avaliações de risco de conformidade para identificar áreas de vulnerabilidade.
- KR2: Desenvolver e implementar estratégias de mitigação de risco que abordem as áreas identificadas.
- KR3: Monitorar continuamente os riscos de conformidade e ajustar as estratégias de mitigação conforme necessário.

Gestão Eficiente de Auditorias

Objetivo: Gerenciar eficientemente todas as atividades relacionadas a auditorias, garantindo transparência e eficácia.

- KR1: Estabelecer um processo padronizado para o agendamento e condução de auditorias internas e externas.
- KR2: Criar um repositório centralizado para armazenar documentos e relatórios de auditorias.
- KR3: Implementar um sistema de acompanhamento de ações corretivas resultantes de auditorias.

Criação de uma Cultura de Conformidade

Objetivo: Promover uma cultura de conformidade dentro da equipe de TI.

- KR1: Realizar treinamentos regulares sobre regulamentos e normas relevantes para sensibilizar a equipe.
- KR2: Estabelecer políticas claras de conformidade e comunicá-las de maneira eficaz.
- KR3: Reconhecer e premiar a conformidade e o compromisso com as políticas de conformidade por meio de programas de incentivo.

Avaliação Contínua e Aprimoramento da Conformidade

Objetivo: Manter um processo de avaliação contínua da conformidade e buscar constantemente melhorias.

- KR1: Realizar avaliações regulares do sistema de conformidade para identificar áreas de aprimoramento.

- KR2: Implementar as melhorias identificadas e medir seu impacto na conformidade.
- KR3: Manter-se atualizado com as mudanças regulatórias e ajustar os controles de conformidade conforme necessário.

Esses OKRs são essenciais para a capability de IT Regulatory, Audit & Compliance Management, pois garantem que a TI esteja em conformidade com todas as obrigações regulatórias e mitigue efetivamente os riscos de conformidade.

Além disso, promovem uma cultura de conformidade dentro da equipe de TI e garantem a eficiência nas atividades de auditoria e avaliação de conformidade.

Critérios para Avaliação de Maturidade

A capability IT Regulatory, Audit & Compliance Management, inserida na macro capability IT Governance e na camada IT Transformation, desempenha um papel essencial na garantia de que a TI esteja em conformidade com leis, regulamentos e normas.

Ela abrange a gestão de auditorias, identificação de riscos de conformidade e a implementação de controles para assegurar o cumprimento das obrigações regulatórias.

A avaliação de maturidade nessa capability é vital para garantir que a organização minimize riscos e mantenha uma postura de conformidade sólida.

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

Nível de Maturidade Inexistente

- Não há conscientização sobre a necessidade de conformidade regulatória na equipe de TI.
- Não existem processos formais para identificar ou monitorar riscos de conformidade.
- Não são realizadas auditorias para verificar a conformidade com regulamentações.

- Não há controles implementados para mitigar riscos de conformidade.
- Não existe documentação sobre as obrigações regulatórias relevantes para a organização.

Nível de Maturidade Inicial

- A conscientização sobre a conformidade regulatória está começando a ser disseminada.
- Processos iniciais para identificar e monitorar riscos de conformidade estão em desenvolvimento.
- Auditorias esporádicas são realizadas para avaliar a conformidade.
- Controles básicos estão sendo implementados para mitigar riscos identificados.
- Uma lista inicial de obrigações regulatórias é documentada.

Nível de Maturidade Definido

- A organização possui políticas e procedimentos documentados relacionados à conformidade regulatória.
- Processos estruturados são usados para identificar e monitorar riscos de conformidade.
- Auditorias regulares são conduzidas e documentadas.
- Controles eficazes são implementados para gerenciar riscos de conformidade.
- Uma lista abrangente de obrigações regulatórias aplicáveis é mantida e atualizada.

Nível de Maturidade Gerenciado

- A conformidade regulatória é uma parte integral da cultura organizacional.
- Processos avançados de identificação e monitoramento de riscos de conformidade são adotados.
- Auditorias são realizadas de forma proativa e resultados são

acompanhados de perto.
- Controles sofisticados e automatizados são implementados para gerenciar riscos de conformidade.
- A organização mantém um registro de conformidade completo e acessível.

Nível de Maturidade Otimizado

- A conformidade regulatória é uma prática de classe mundial na organização.
- A identificação e o monitoramento de riscos de conformidade são altamente eficazes.
- Auditorias são conduzidas de forma contínua e resultados são usados para aprimorar processos.
- Controles são constantemente otimizados e a automação é maximizada.
- A organização mantém um registro de conformidade altamente sofisticado, com análises avançadas para prever riscos futuros.

A avaliação de maturidade na capability IT Regulatory, Audit & Compliance Management é crítica para assegurar que a organização esteja em conformidade com regulamentações e normas relevantes, protegendo-se contra riscos legais e financeiros.

À medida que a maturidade aumenta, a organização pode alcançar níveis mais altos de eficiência e eficácia na gestão de conformidade regulatória.

Convergência com Frameworks de Mercado

A capability IT Regulatory, Audit & Compliance Management, integrante da macro capability IT Governance e da camada IT Transformation, é vital para assegurar a aderência da área de TI às leis, regulamentos e normas.

Esta capability engloba a gestão de auditorias, a identificação de riscos de conformidade e a implementação de controles necessários para cumprir as obrigações regulatórias.

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 oferece um forte alinhamento com esta capability, visto que enfatiza a governança e a gestão de TI, incluindo conformidade e riscos. A sua abordagem estruturada para a governança de TI ressalta a importância da conformidade regulatória e auditorias, demonstrando alta convergência.

ITIL

- Nível de Convergência: Médio
- Racional: O ITIL, focado na gestão de serviços de TI, aborda aspectos de conformidade e auditoria em suas práticas, embora não seja seu foco principal. A conformidade é considerada importante para a entrega eficaz de serviços, resultando numa convergência média.

SAFe

- Nível de Convergência: Baixo
- Racional: O SAFe, sendo um framework ágil, tem menos ênfase na conformidade regulatória e auditoria. Seu foco está mais no desenvolvimento ágil e entrega de valor, levando a uma convergência baixa com esta capability.

PMI

- Nível de Convergência: Médio
- Racional: O PMI reconhece a importância da conformidade regulatória e auditoria no gerenciamento de projetos, mas não é o foco central do

framework. Estes aspectos são considerados no contexto do gerenciamento de riscos e governança de projetos.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI, focado na melhoria de processos, incorpora a conformidade e auditoria como parte da gestão de qualidade e riscos. Ainda que não seja o foco primário, a conformidade é importante para alcançar a maturidade dos processos.

TOGAF

- Nível de Convergência: Baixo
- Racional: O TOGAF, voltado para a arquitetura empresarial, tem um foco limitado em conformidade regulatória e auditoria. Estes aspectos são mais relevantes no contexto da implementação de soluções de TI alinhadas às necessidades empresariais.

DevOps SRE

- Nível de Convergência: Baixo
- Racional: O DevOps SRE concentra-se na entrega contínua e na confiabilidade dos serviços, com menos ênfase em conformidade e auditoria. Seu foco principal está na eficiência operacional e na melhoria contínua.

NIST

- Nível de Convergência: Alto
- Racional: O NIST, com seu enfoque em padrões de segurança e conformidade, tem uma alta convergência com esta capability. A conformidade com os padrões NIST é fundamental para muitas organizações, especialmente em contextos regulados.

Six Sigma

- Nível de Convergência: Médio
- Racional: O Six Sigma, focado na melhoria da qualidade e eficiência, considera a conformidade e auditoria no contexto da redução de erros e melhoria dos processos. Embora não seja o foco principal, a conformidade é um aspecto relevante.

Lean IT

- Nível de Convergência: Baixo
- Racional: Lean IT, voltado para a eficiência e eliminação de desperdícios, tem um enfoque limitado em conformidade regulatória e auditoria. Estes aspectos são secundários em relação ao objetivo principal de maximizar o valor através da eficiência.

A capability IT Regulatory, Audit & Compliance Management desempenha um papel fundamental na garantia de que a TI opere dentro dos parâmetros legais e regulamentares.

A sua integração com diferentes frameworks de mercado reflete sua importância estratégica, assegurando que as atividades de TI estejam alinhadas não apenas com os objetivos organizacionais, mas também com as exigências regulatórias e de auditoria.

Processos e Atividades

Develop Compliance Strategy

Desenvolver uma estratégia de conformidade para TI alinhada com os objetivos do negócio é essencial para garantir que todas as operações de TI estejam em conformidade com as leis e regulamentos aplicáveis.

Este processo envolve a criação de um plano abrangente que aborde todas as áreas críticas de conformidade, incluindo privacidade de dados, segurança cibernética e

requisitos de auditoria.

A estratégia deve considerar os riscos específicos enfrentados pela organização e definir medidas preventivas e corretivas.

Além disso, é necessário identificar os recursos necessários, tanto humanos quanto tecnológicos, e estabelecer um cronograma para a implementação das iniciativas de conformidade.

A comunicação clara da estratégia e o treinamento adequado dos colaboradores são fundamentais para assegurar o cumprimento das políticas estabelecidas.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Assess Compliance Landscape	Avaliar o panorama regulatório e de conformidade relevante para a organização.	Leis e regulamentos aplicáveis, benchmarks	Relatório de avaliação do panorama regulatório	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 Compliance Objectives	Definir os objetivos de conformidade alinhados com os objetivos do negócio.	Feedback de stakeholders, análise de riscos	Objetivos de conformidade 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 Compliance Policies	Desenvolver políticas de conformidade detalhadas e alinhadas com os objetivos definidos.	Objetivos de conformidade, benchmark de políticas	Políticas de conformidade 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 Compliance Framework	Estabelecer um framework de conformidade que suporte a implementação das políticas.	Políticas de conformidade, frameworks de referência	Framework de conformidade 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 Compliance Strategy	Comunicar a estratégia de conformidade para todas as partes interessadas.	Framework de conformidade, políticas de conformidade	Estratégia de conformidade 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 Regulatory Requirements

Identificar os requisitos regulatórios aplicáveis à organização é um processo crítico para assegurar que todas as operações de TI estejam em conformidade com as leis e regulamentos pertinentes.

Este processo envolve a pesquisa e análise detalhada dos regulamentos locais, nacionais e internacionais que impactam a organização.

A identificação de requisitos regulatórios abrange áreas como proteção de dados, segurança da informação, privacidade e auditorias.

A colaboração com departamentos legais e consultores externos pode ser necessária para garantir uma compreensão abrangente das obrigações regulatórias.

Uma vez identificados, esses requisitos devem ser documentados e comunicados às partes interessadas para garantir a conformidade contínua.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Research Regulatory Landscape	Pesquisar o cenário regulatório aplicável à organização.	Leis e regulamentos, consulta a especialistas	Relatório de pesquisa regulatória	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Legal; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Legal; Recommender: Cybersecurity; Executer: IT Governance & Transformation
2	Identify Applicable Regulations	Identificar os regulamentos específicos que impactam a organização.	Relatório de pesquisa regulatória	Lista de regulamentos aplicáveis	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Legal; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Legal; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation

3	Analyze Compliance Impact	Analisar o impacto dos regulamentos na organização e suas operações de TI.	Lista de regulamentos aplicáveis	Análise de impacto regulatório	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Legal; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation
4	Document Regulatory Requirements	Documentar os requisitos regulatórios identificados.	Análise de impacto regulatório	Documento de requisitos regulatórios	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Legal; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Legal; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation
5	Communicate Requirements	Comunicar os requisitos regulatórios para todas as partes interessadas relevantes.	Documento de requisitos regulatórios	Requisitos comunicados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Legal; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation

Implement Compliance Programs

Implementar programas de conformidade é crucial para garantir que a organização adira às políticas e regulamentações estabelecidas.

Este processo envolve a criação e execução de programas que abrangem treinamento, monitoramento e auditoria das práticas de conformidade.

A implementação deve incluir a designação de responsáveis por cada aspecto do programa, a criação de processos claros para o reporte e a resolução de não conformidades, e a integração de tecnologias que facilitem o monitoramento contínuo.

Além disso, a comunicação e o treinamento são fundamentais para garantir que todos os colaboradores compreendam suas responsabilidades e estejam preparados para cumprir os requisitos de conformidade.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Design Compliance Programs	Desenhar programas de conformidade alinhados com os requisitos regulatórios.	Requisitos regulatórios, políticas de conformidade	Programas de conformidade desenhados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Legal; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
2	Assign Compliance Roles	Designar responsáveis por cada aspecto dos programas de conformidade.	Programas de conformidade desenhados	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	Develop Training Programs	Desenvolver programas de treinamento para assegurar a compreensão das políticas de conformidade.	Programas de conformidade, políticas de conformidade	Programas de treinamento desenvolvidos	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	Implement Monitoring Tools	Implementar ferramentas de monitoramento para assegurar a conformidade contínua.	Programas de conformidade, ferramentas de monitoramento	Ferramentas de monitoramento implementadas	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	Execute Compliance Programs	Executar os programas de conformidade, monitorando continuamente a aderência.	Ferramentas de monitoramento, programas de conformidade	Conformidade monitorada	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 Compliance Performance

Monitorar continuamente o desempenho dos programas de conformidade utilizando indicadores-chave de desempenho (KPIs) é vital para assegurar a eficácia e a aderência às políticas regulatórias.

Este processo envolve a coleta e análise de dados de conformidade, a fim de identificar possíveis desvios e áreas de melhoria.

A definição de KPIs claros e mensuráveis permite uma avaliação objetiva do desempenho de conformidade.

O monitoramento contínuo inclui a realização de auditorias internas regulares e a implementação de sistemas de alerta para não conformidades.

A comunicação dos resultados para as partes interessadas é fundamental para garantir a transparência e a tomada de ações corretivas quando necessário.

- PDCA focus: Check
- Periodicidade: Trimestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Define Compliance KPIs	Definir indicadores-chave de desempenho para monitorar a conformidade.	Requisitos regulatórios, programas de conformidade	KPIs definidos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Legal; Recommender: Cybersecurity; Executer: IT Governance & Transformation
2	Collect Compliance Data	Coletar dados de desempenho relacionados à conformidade.	Ferramentas de monitoramento, relatórios de auditoria	Dados de conformidade coletados	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
3	Analyze Compliance Performance	Analisar os dados coletados para avaliar a conformidade com os KPIs definidos.	Dados de conformidade coletados	Análise de desempenho de conformidade	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

4	Conduct Compliance Audits	Realizar auditorias internas de conformidade para validar os resultados.	Análise de desempenho de conformidade	Relatórios de auditoria de conformidade	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
5	Communicate Compliance Results	Comunicar os resultados das auditorias e análises de desempenho para as partes interessadas.	Relatórios de auditoria de conformidade	Resultados de conformidade comunicados	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

Review and Update Compliance Processes

Revisar e atualizar os processos de conformidade com base nos resultados das auditorias e feedbacks recebidos é essencial para assegurar a melhoria contínua e a eficácia dos programas de conformidade.

Este processo envolve a análise crítica dos resultados das auditorias, a identificação de áreas de melhoria e a implementação de mudanças necessárias.

A revisão deve considerar as melhores práticas do setor e as lições aprendidas de ciclos anteriores para garantir que os processos de conformidade estejam sempre atualizados e alinhados com os requisitos regulatórios.

A comunicação das atualizações é fundamental para garantir que todas as partes interessadas estejam cientes das mudanças e possam se adaptar adequadamente.

- PDCA focus: Act
- Periodicidade: Semestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Evaluate Audit Results	Avaliar criticamente os resultados das auditorias de conformidade.	Relatórios de auditoria de conformidade	Relatório de avaliação de auditoria	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	Identify Improvement Areas	Identificar áreas de melhoria nos processos de conformidade.	Relatório de avaliação de auditoria	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 conformidade.	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 conformidade 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