



Convergência com Frameworks de Mercado



The IT Framework
www.ciocodex.com

Convergência com Frameworks de Mercado

A capability Cybersecurity Governance, pertencente à macro capability Definition & Management e integrada na camada Cybersecurity, é crucial para assegurar que as políticas, procedimentos e controles de segurança estejam em conformidade com

regulamentações e padrões da indústria.

Esta capability envolve o monitoramento do cumprimento das políticas de segurança e a avaliação contínua dos riscos de segurança, garantindo uma postura de segurança eficaz e atualizada.

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

;

COBIT

· Nível de Convergência: Alto

· Racional: O COBIT destaca a governança de TI, incluindo a segurança cibernética. A Cybersecurity Governance é essencial para cumprir com os padrões do COBIT, assegurando que a governança da segurança cibernética esteja alinhada com os objetivos organizacionais e os processos de governança.

;

ITIL

· Nível de Convergência: Médio

· Racional: O ITIL enfoca a gestão de serviços de TI, incluindo aspectos de segurança. A Cybersecurity Governance complementa o ITIL ao integrar práticas de segurança nos processos de gestão de serviços e no gerenciamento de riscos associados.

;

SAFe

· Nível de Convergência: Médio

· Racional: O SAFe concentra-se em agilidade e desenvolvimento de software. Embora a governança de segurança cibernética não seja um foco direto, ela suporta o SAFe ao garantir a segurança nos ciclos de desenvolvimento e entrega.

;

PMI

· Nível de Convergência: Médio

· Racional: O PMI aborda amplamente a gestão de projetos, onde a governança de segurança cibernética pode desempenhar um papel importante na minimização de riscos relacionados à segurança em projetos de TI.

;

CMMI

· Nível de Convergência: Médio

· Racional: O CMMI visa a maturidade e a melhoria dos processos. A Cybersecurity Governance auxilia no alcance de uma maturidade maior em segurança, influenciando positivamente a avaliação de riscos e a gestão de processos de TI.

;

TOGAF

· Nível de Convergência: Alto

· Racional: O TOGAF foca na arquitetura empresarial, onde a governança de segurança cibernética é crucial. A Cybersecurity Governance assegura que a segurança seja uma parte integrante da arquitetura de TI e dos processos de tomada de decisão.

;

DevOps SRE

· Nível de Convergência: Médio

· Racional: Em DevOps e SRE, a segurança é frequentemente integrada ao ciclo de vida do desenvolvimento. A governança de segurança cibernética reforça esta integração, promovendo práticas seguras de desenvolvimento e operações.

;

NIST

· Nível de Convergência: Alto

· Racional: O NIST fornece diretrizes detalhadas para a segurança cibernética. A Cybersecurity Governance está fortemente alinhada ao NIST, ao estabelecer um framework para a implementação de controles de segurança eficazes e gerenciamento de riscos.

;

Six Sigma

· Nível de Convergência: Baixo

· Racional: O Six Sigma concentra-se na melhoria da qualidade e redução de defeitos. A Cybersecurity Governance, embora não seja um foco direto do Six Sigma, pode contribuir para a melhoria da qualidade através da redução de riscos e

vulnerabilidades de segurança.

;

Lean IT

· Nível de Convergência: Baixo

· Racional: Lean IT enfatiza a eficiência operacional, enquanto a Cybersecurity Governance se concentra mais na segurança. Apesar disso, uma governança de segurança eficaz pode contribuir para a eficiência ao prevenir interrupções e perdas relacionadas à segurança.

;

A Cybersecurity Governance é fundamental no contexto atual, onde as ameaças cibernéticas são uma realidade constante.

Ela não apenas fortalece a segurança da informação e dos sistemas de uma organização, mas também assegura que as práticas de segurança estejam em sintonia com os objetivos estratégicos e operacionais.

KPIs relevantes para esta capability incluem a taxa de conformidade com as políticas de segurança, o tempo de resposta a incidentes de segurança e a eficácia das medidas preventivas implementadas.

A estratégia de cibersegurança eficazmente implementada e gerida não apenas eleva a maturidade da organização em termos de segurança, mas também apoia a sua resiliência operacional e a capacidade de resposta a ameaças emergentes.

;



CIO Codex

Com o advento da era digital, a Tecnologia da Informação assumiu um papel de destaque dentro das estratégias corporativas das empresas dos mais diversos portes e setores de atuação. O CIO Codex Framework foi concebido com o propósito de oferecer uma visão integrada dos conceitos de uma área de tecnologia pronta para a era digital.



The IT framework

O conteúdo apresentado neste website, incluindo o framework, é protegido por direitos autorais e é de propriedade exclusiva do CIO Codex. Isso inclui, mas não se limita a, textos, gráficos, marcas, logotipos, imagens, vídeos e demais materiais disponíveis no site. Qualquer reprodução, distribuição, ou utilização não autorizada desse conteúdo é estritamente proibida e sujeita às penalidades previstas na legislação aplicável