Cibersegurança

Topical Requirement

Requisito Temático

The Institute of
Internal Auditors

Requisito Temático de Cibersegurança

O Framework Internacional de Práticas Profissionais (International Professional Practices Framework®) comprehende as Normas Globais de Auditoria Interna (Global Internal Audit Standards™) e as Orientações Globais. Os Requisitos Temáticos são obrigatórios e devem ser usados em conjunto com as Normas, que fornecem a base de autoridade para as práticas exigidas.

Os Requisitos Temáticos fornecem expectativas claras para os auditores internos, definindo uma linha de base mínima para a auditoria de temas de risco especificados. O perfil de risco da organização pode exigir que os auditores internos considerem aspectos adicionais do tema.

A conformidade com os Requisitos Temáticos aumentará a consistência com a qual os serviços de auditoria interna são executados e melhorará a qualidade e a confiabilidade dos serviços e resultados de auditoria interna. Em última análise, os Requisitos Temáticos elevam a profissão de auditoria interna.

Os auditores internos devem aplicar os Requisitos Temáticos em conformidade com as Normas Globais de Auditoria Interna. A conformidade com os Requisitos Temáticos é obrigatória para serviços de avaliação e recomendada para serviços de consultoria.

O Requisito Temático é aplicável quando o tema é um dos seguintes:

A. Assunto de um trabalho no plano de auditoria interna.
B. Identificado durante a execução de um trabalho.
C. Objeto de uma solicitação de trabalho que não consta no plano de auditoria interna original.

As evidências de que a aplicabilidade de cada requisito do Requisito Temático foi avaliada devem ser documentadas e guardadas. Nem todos os requisitos individuais podem ser aplicados em todos os trabalhos; se requisitos forem excluídos, uma justificativa deve ser documentada e guardada. A conformidade com o Requisito Temático é obrigatória e será avaliada durante as avaliações de qualidade.

Para mais informações, consulte o Guia do Usuário do Requisito Temático de Cibersegurança.

Cibersegurança

O National Institute of Standards and Technology (NIST) define a cibersegurança simplesmente como "a capacidade de proteger ou defender o uso do espaço cibernético contra ciberataques". A cibersegurança é um subconjunto da segurança da informação abrangente, que o NIST define como "a proteção de informações e sistemas de informação contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados, a fim de fornecer confidencialidade, integridade e disponibilidade".

A cibersegurança reduz o risco ao fortalecer o ambiente geral de controle e proteger os ativos de informação de uma organização contra acesso não autorizado, interrupção, alteração ou destruição. Os ciberataques podem levar a impactos diretos e indiretos, que geralmente são significativos, pois computadores, redes, programas, dados e informações confidenciais são componentes essenciais da maioria das organizações.

Analisando e Avaliando os Processos de Governança, Gerenciamento de Riscos e Controle de Cibersegurança

Este requisito temático fornece uma abordagem consistente e abrangente para avaliar a criação e a implementação dos processos de governança, gerenciamento de riscos e controle da cibersegurança. Os requisitos representam uma linha de base mínima para avaliar a cibersegurança em uma organização.

GOVERNANÇA: Analisando e Avaliando a Governança da Cibersegurança

Requisitos:

Os auditores internos devem avaliar o seguinte em relação à governança da cibersegurança da organização:

A. São estabelecidos uma estratégia e objetivos formais de cibersegurança, atualizados periodicamente. As atualizações sobre a concretização dos objetivos de cibersegurança são periodicamente comunicadas e revisadas pelo conselho, incluindo recursos e considerações orçamentárias para apoiar a estratégia de cibersegurança.
B. Políticas e procedimentos relacionados à cibersegurança são estabelecidos e atualizados periodicamente, para fortalecer o ambiente de controle.
C. São estabelecidos papéis e responsabilidades que apoiam os objetivos de cibersegurança e existe um processo para avaliar periodicamente o conhecimento, as habilidades e as capacidades dos indivíduos que desempenham esses papéis.
D. Os stakeholders relevantes são envolvidos, para discutir e agir quanto às vulnerabilidades existentes e às ameaças emergentes no ambiente de cibersegurança. Os stakeholders incluem a alta administração, as operações, o gerenciamento de riscos, os recursos humanos, o departamento jurídico, a conformidade, os fornecedores e outros.

GERENCIAMENTO DE RISCOS: Analisando e Avaliando o Gerenciamento de Riscos de Cibersegurança

Requisitos:

Os auditores internos devem avaliar o seguinte em relação ao gerenciamento de riscos de cibersegurança da organização:

A. Os processos de avaliação e gerenciamento de riscos da organização incluem a identificação, análise, mitigação e monitoramento das ameaças à cibersegurança e seu efeito sobre a concretização dos objetivos estratégicos.
B. O gerenciamento de riscos de cibersegurança é realizado em toda a organização e pode incluir as seguintes áreas: tecnologia da informação, gerenciamento de riscos corporativos, recursos humanos, jurídico, conformidade, operações, cadeia de suprimentos, contabilidade, finanças e outras.
C. São estabelecidas prestação de contas e responsabilidades pelo gerenciamento de riscos de cibersegurança. Um indivíduo ou equipe é identificado para monitorar e reportar periodicamente como os riscos de cibersegurança estão sendo gerenciados, incluindo os recursos necessários para mitigar os riscos e identificar ameaças emergentes à cibersegurança.
D. Um processo é estabelecido para escalar rapidamente qualquer risco de cibersegurança (emergente ou previamente identificado) que atinja um nível inaceitável de acordo com as diretrizes de gerenciamento de riscos estabelecidas pela organização ou com os requisitos legais e regulatórios aplicáveis. Os impactos financeiros e não financeiros do risco de cibersegurança deveriam ser considerados.
E. Foi estabelecido um processo para conscientizar a gestão e os funcionários sobre os riscos de cibersegurança e para a gestão analisar periodicamente problemas, lacunas, deficiências ou falhas de controle com relatórios e correções tempestivos.
F. A organização implementou um processo de resposta e recuperação após incidentes de cibersegurança que inclui detecção, contenção, recuperação e análise pós-incidente. O processo de resposta e recuperação após incidentes é testado periodicamente.

CONTROLES: Analisando e Avaliando os Processos de Controle de Cibersegurança

Requisitos:

Os auditores internos devem avaliar o seguinte em relação aos processos de controle de cibersegurança da organização:

A. Um processo é estabelecido para garantir que controles internos e controles de fornecedores estejam em vigor, para proteger a confidencialidade, a integridade e a disponibilidade dos sistemas e dados da organização. Avaliações são realizadas periodicamente para determinar se os controles estão funcionando de forma a promover a concretização dos objetivos de cibersegurança da organização e a resolução imediata de problemas.

B. É estabelecido um processo de gestão de talentos que inclui treinamento para desenvolver e manter as competências técnicas relacionadas às operações de cibersegurança. O processo é revisado periodicamente.

C. É estabelecido um processo para monitorar e reportar continuamente as ameaças e vulnerabilidades emergentes de cibersegurança e para identificar, priorizar e implementar oportunidades de melhoria para as operações de cibersegurança.

D. A cibersegurança está incluída no gerenciamento do ciclo de vida (seleção, uso, manutenção e desativação) de todos os ativos de TI, inclusive hardware, software e serviços de fornecedores.

E. São estabelecidos processos para fortalecer a cibersegurança, incluindo configuração, administração de dispositivos do usuário final, criptografia, aplicação de patches, gerenciamento de acesso do usuário e monitoramento da disponibilidade e do desempenho. Considerações de cibersegurança são incluídas no desenvolvimento de software (DevSecOps).

F. São estabelecidos controles relacionados à rede, como controles de acesso à rede e segmentação; uso e posicionamento de firewalls; conexões limitadas de e para redes externas; rede privada virtual (VPN)/acesso à rede de confiança zero (ZTNA); controles de rede da Internet das Coisas (IoT); e sistemas de detecção/prevenção de intrusão (IDS e IPS).

G. São estabelecidos controles de segurança de comunicação de *endpoint* para serviços como e-mail, navegadores de Internet, videoconferência, mensagens, redes sociais, nuvem e protocolos de compartilhamento de arquivos.

Sobre o Instituto de Auditores Internos

O Institute of Internal Auditors (The IIA) é uma associação profissional internacional que atende a mais de 255.000 membros globais e concedeu mais de 200.000 certificações *Certified Internal Auditor*® (CIA®) em todo o mundo. Fundado em 1941, o The IIA é reconhecido no mundo todo como o líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para mais informações, acesse www.theiia.org.

Copyright

Fevereiro de 2025

The Institute of Internal Auditors

Sede global
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, EUA
Telefone: +1-407-937-1111
Fax: +1-407-937-1101